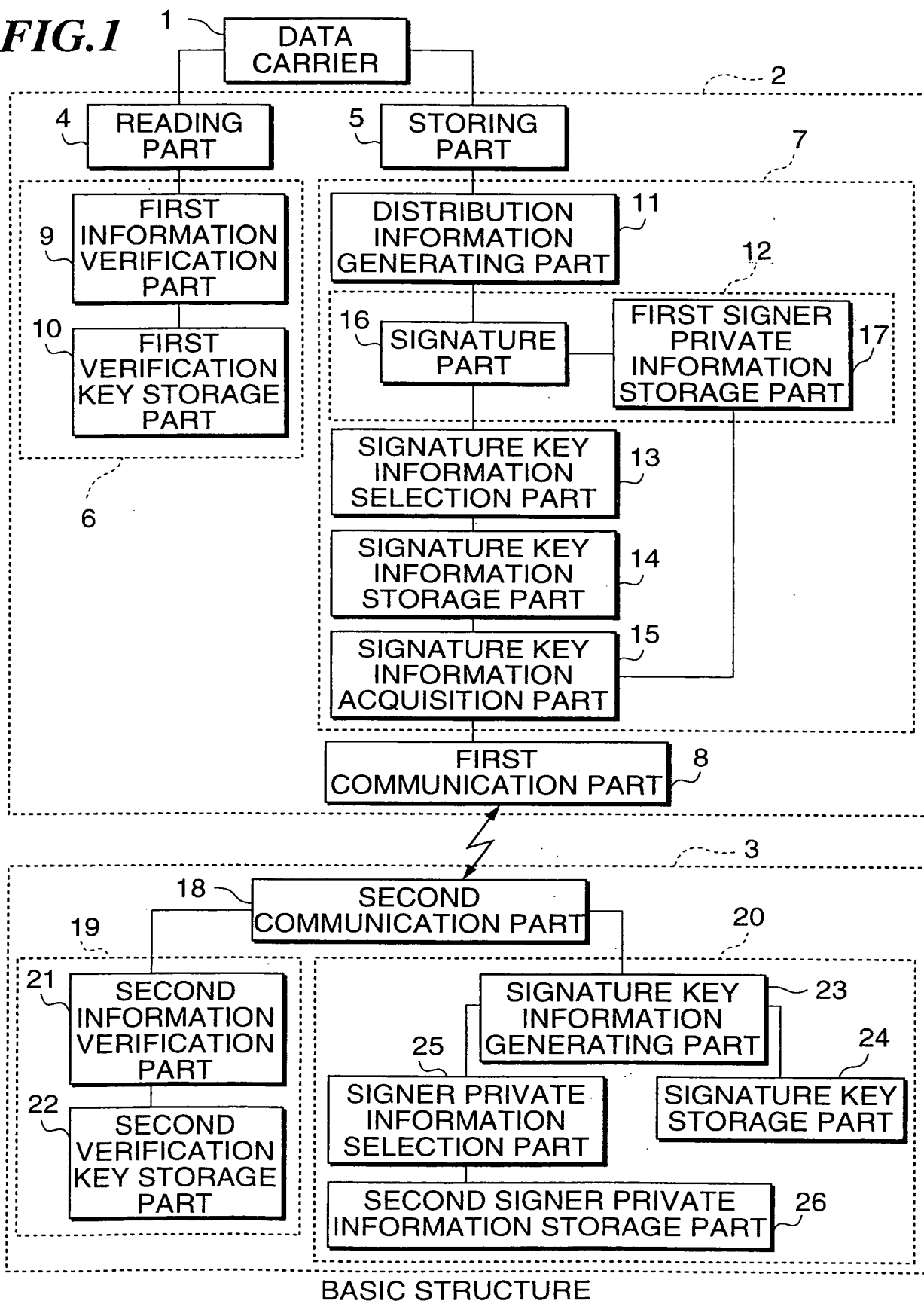
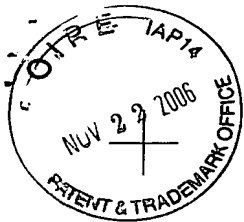


1/34

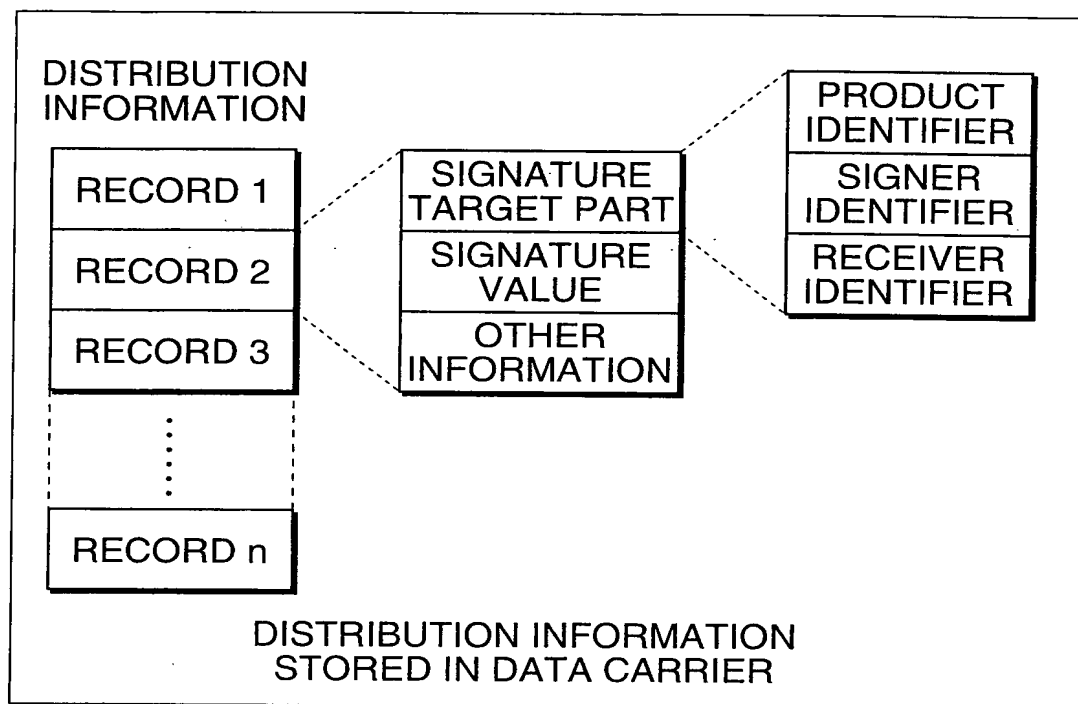
FIG.1

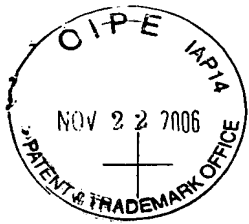




2/34

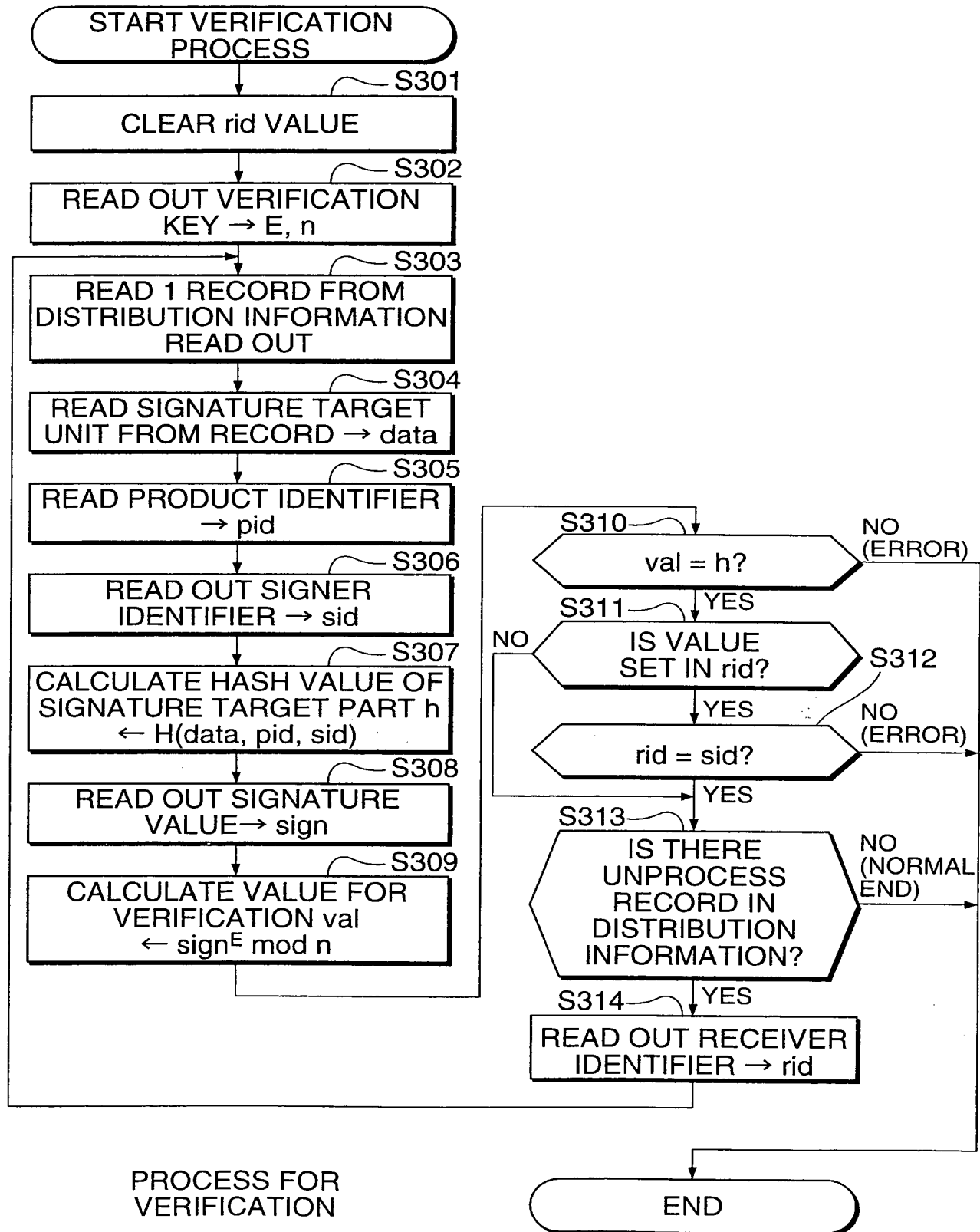
FIG.2

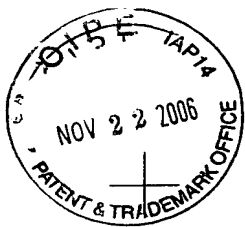




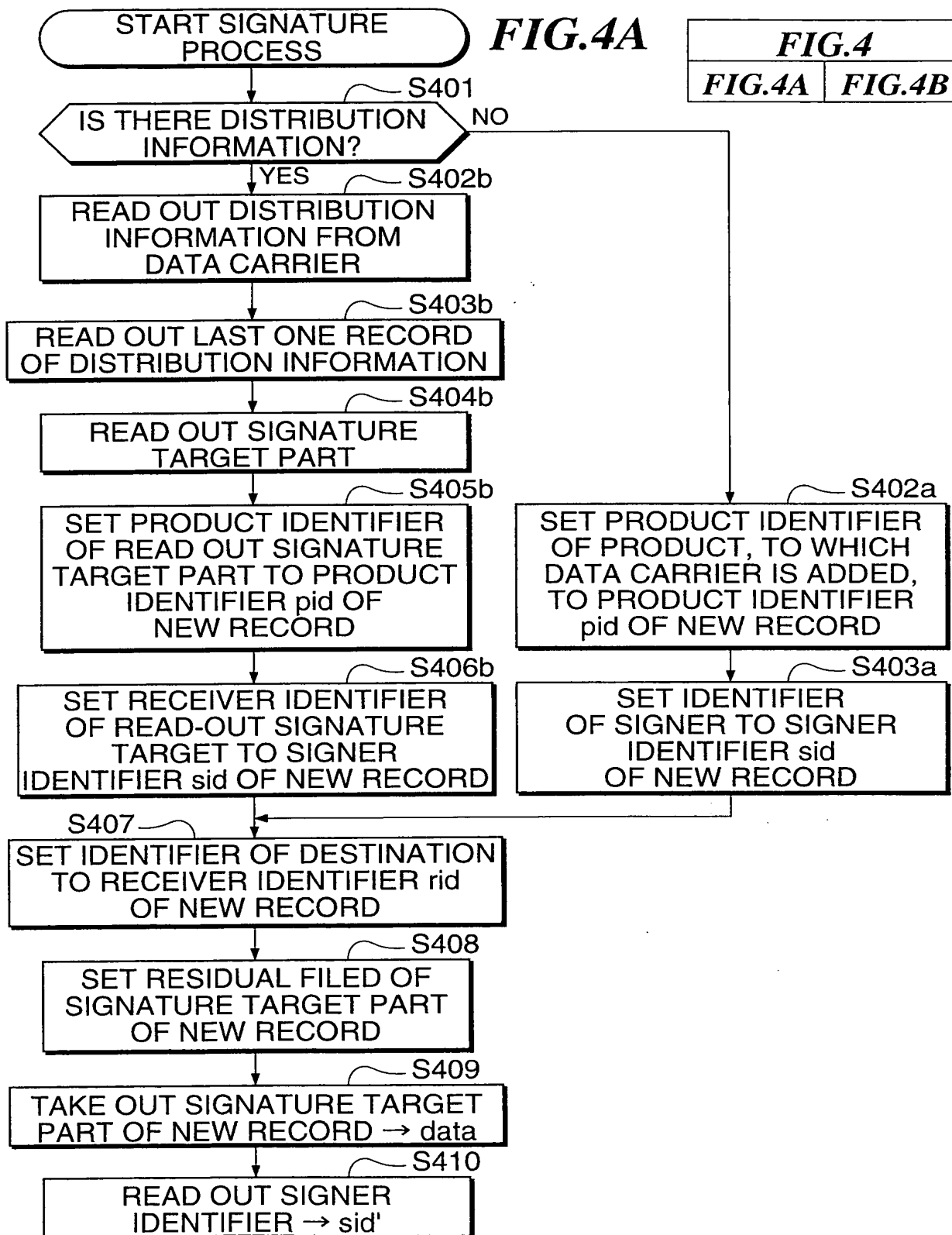
3/34

FIG.3





4/34



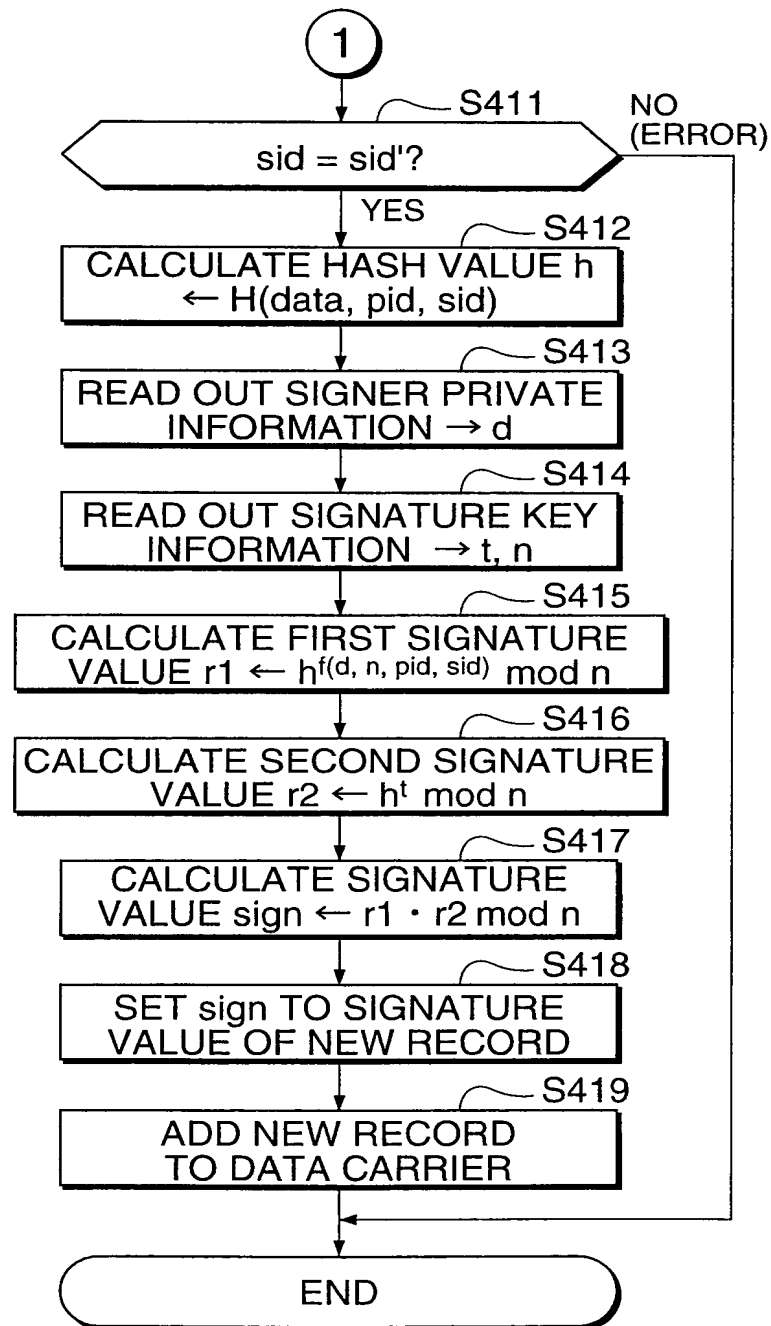
1

PROCESS FOR SIGNING



5/34

FIG.4B



PROCESS FOR SIGNING



FIG.5A

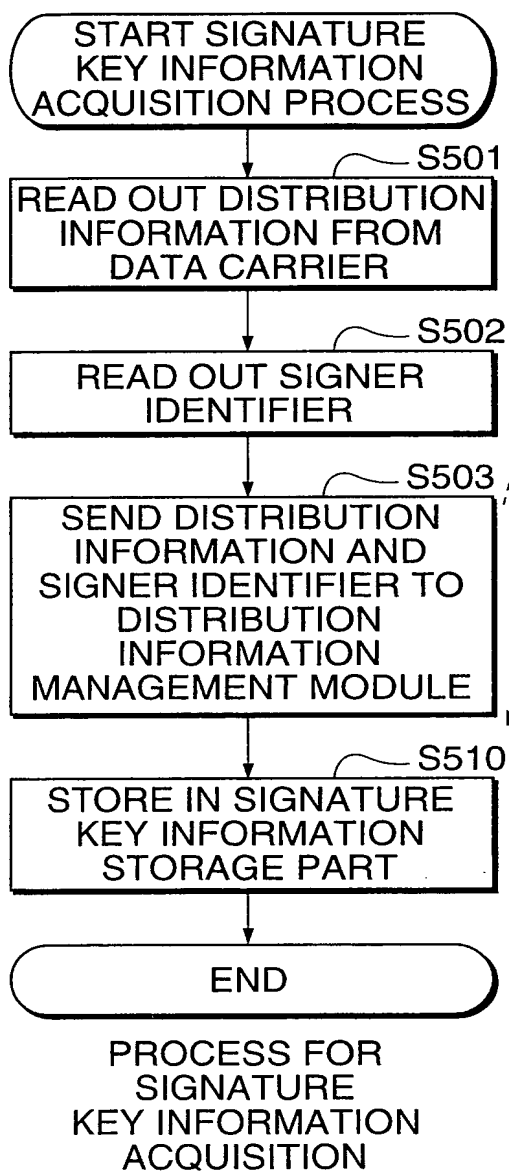


FIG.5B

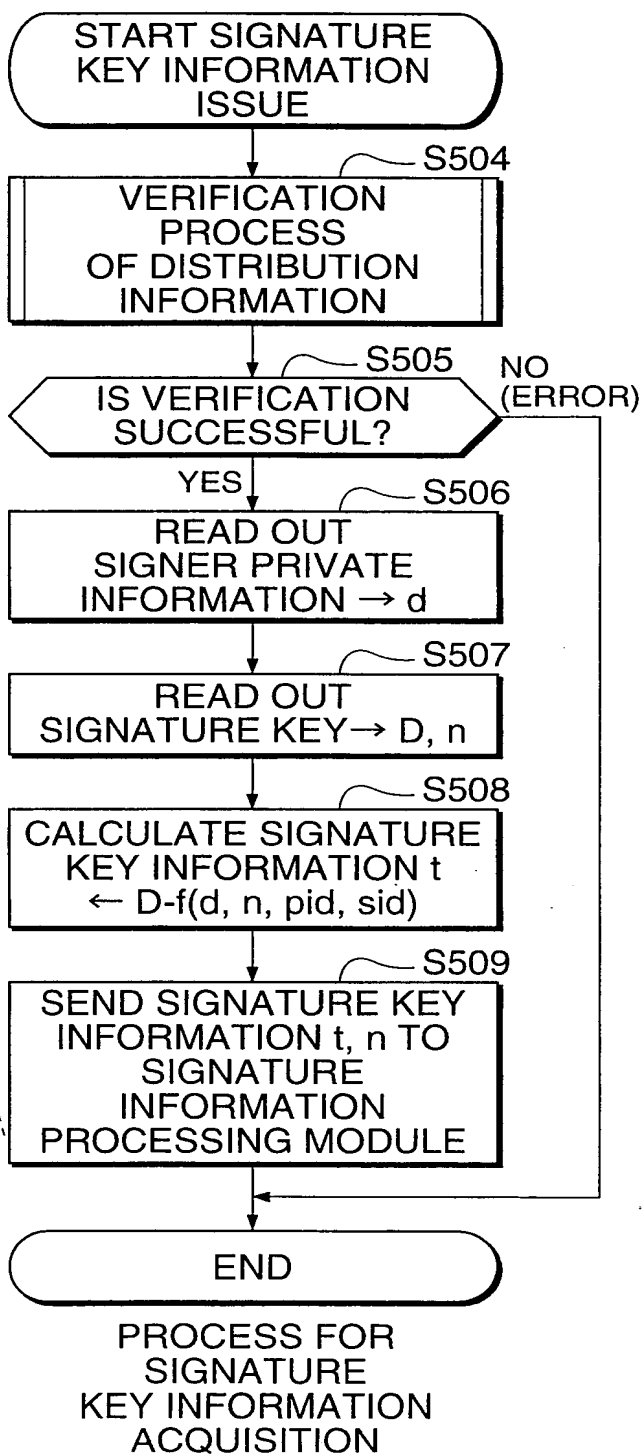




FIG.6

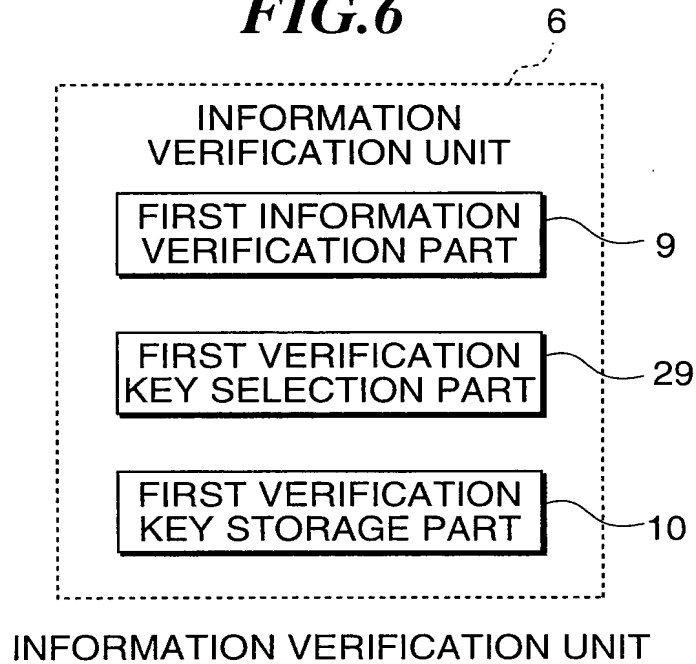


FIG.7

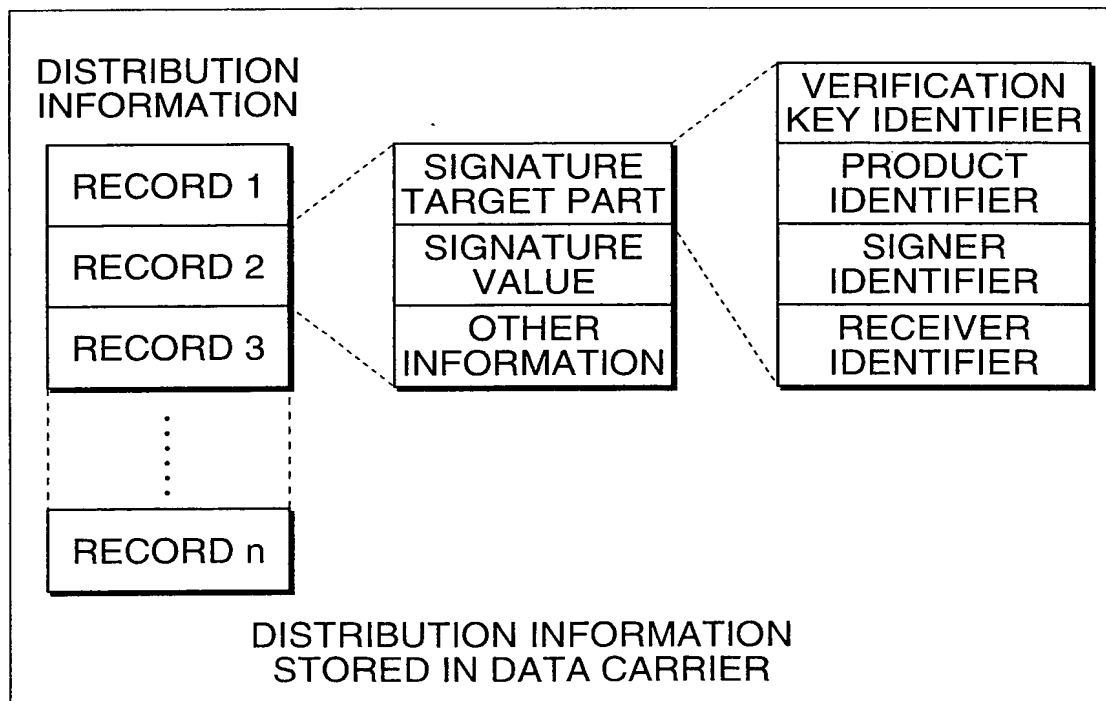
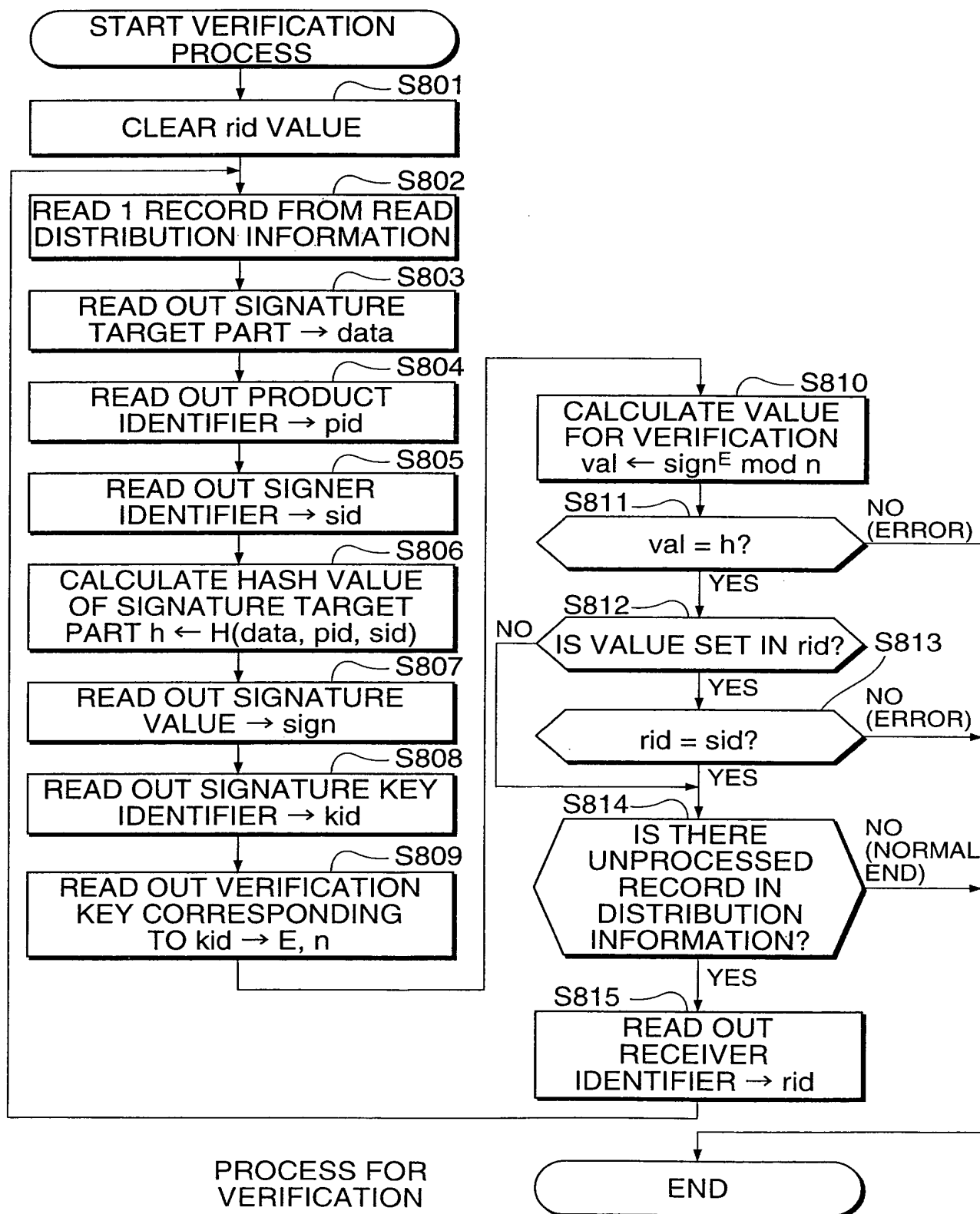


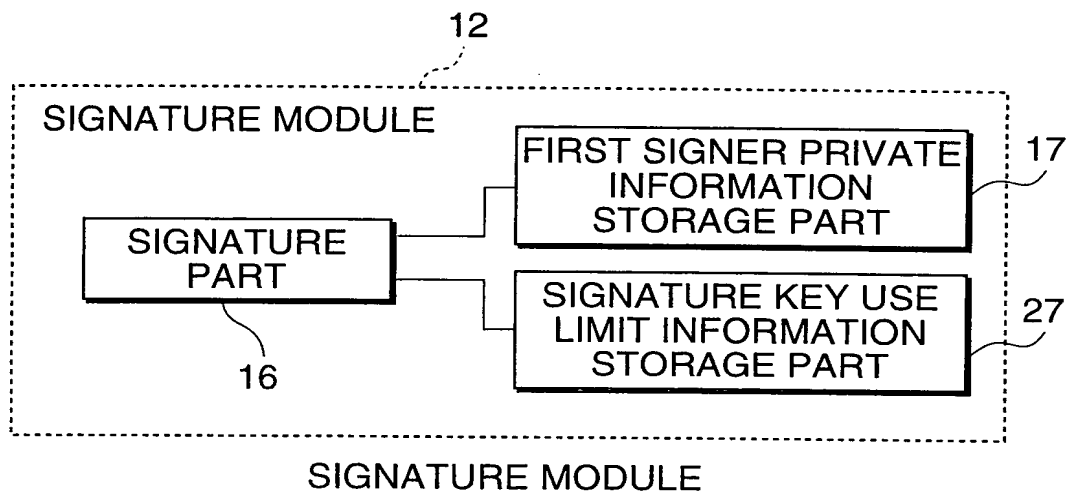
FIG.8





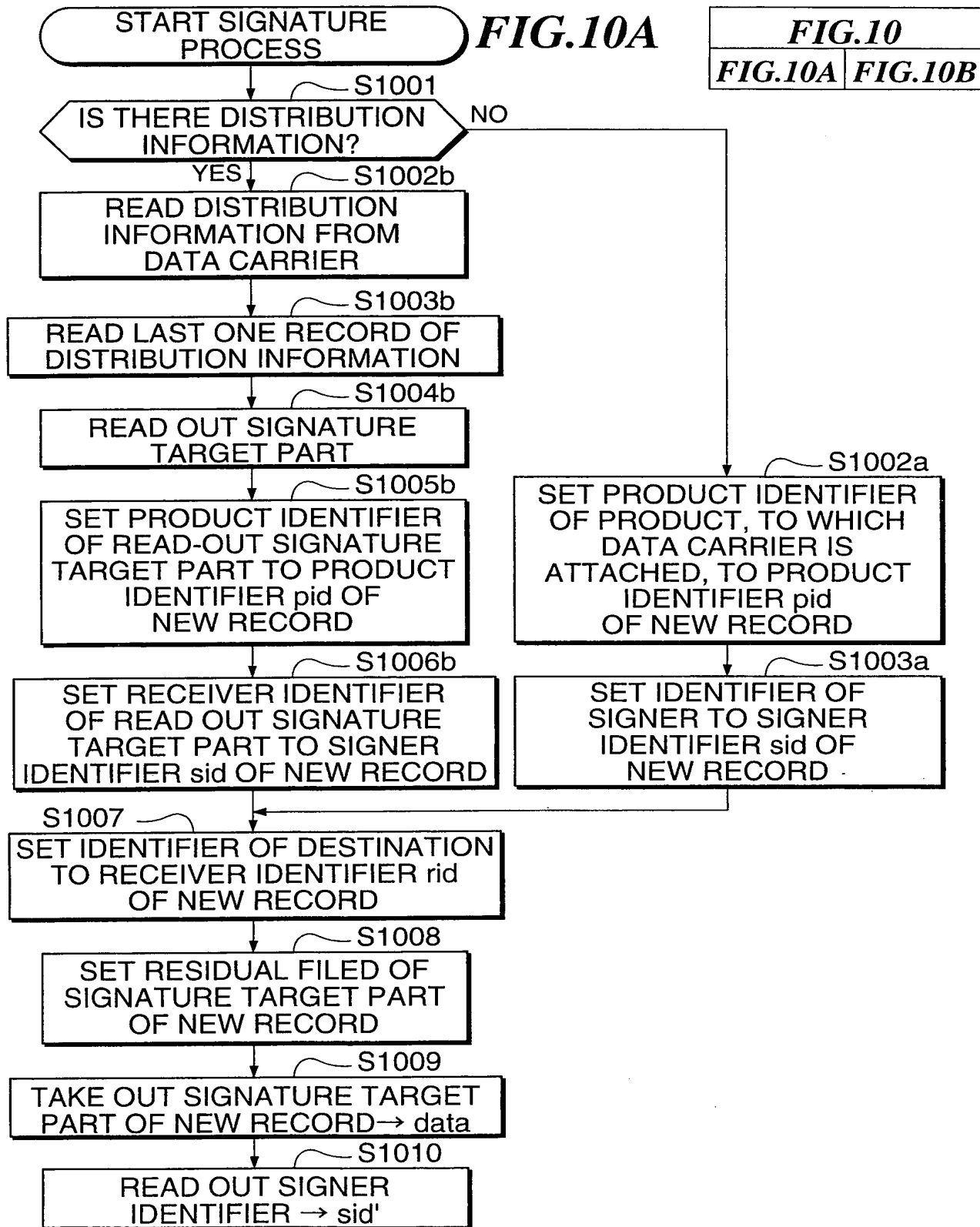
9/34

FIG. 9





10/34



1

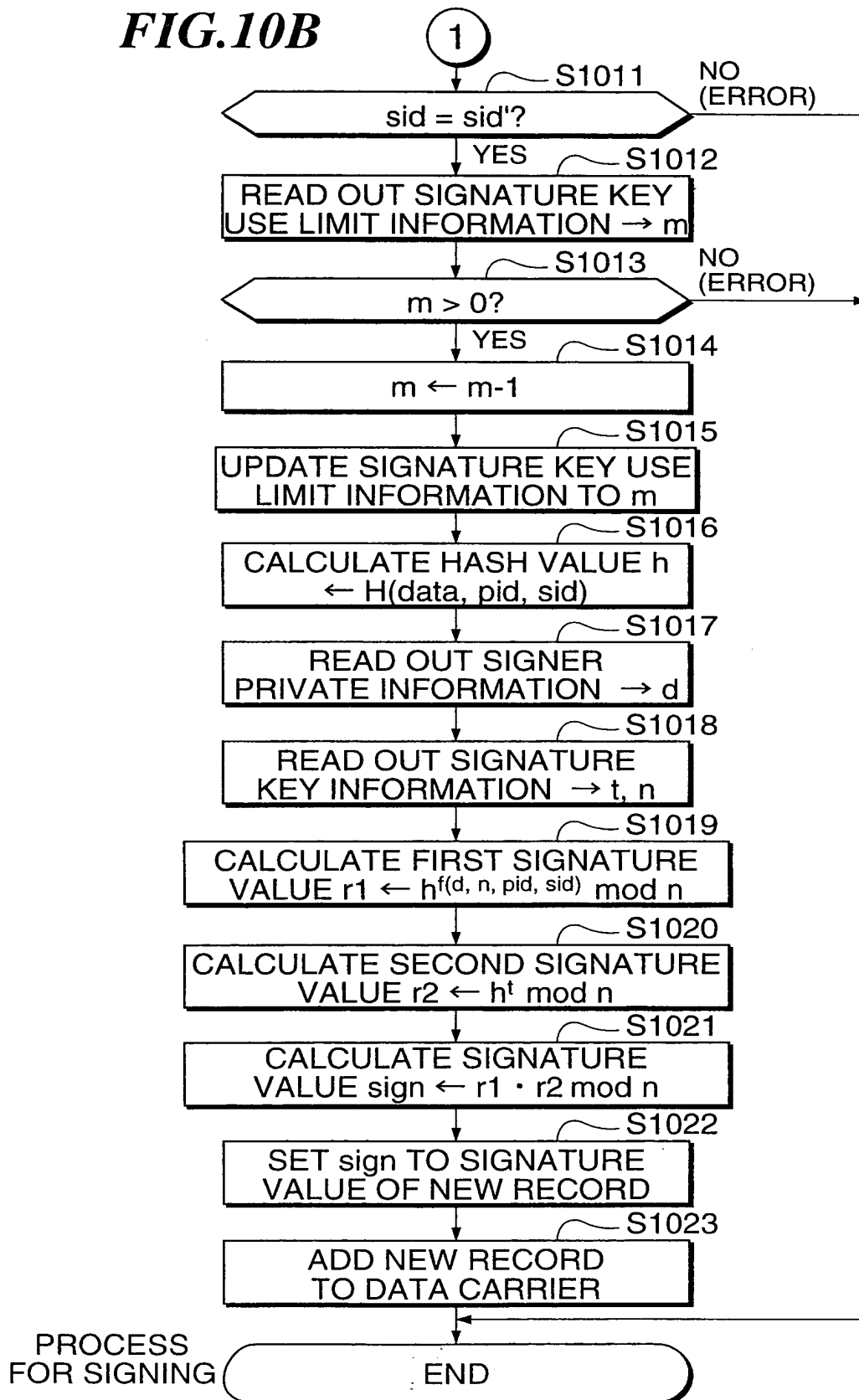
PROCESS FOR SIGNING

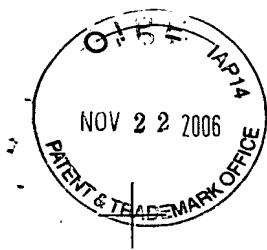




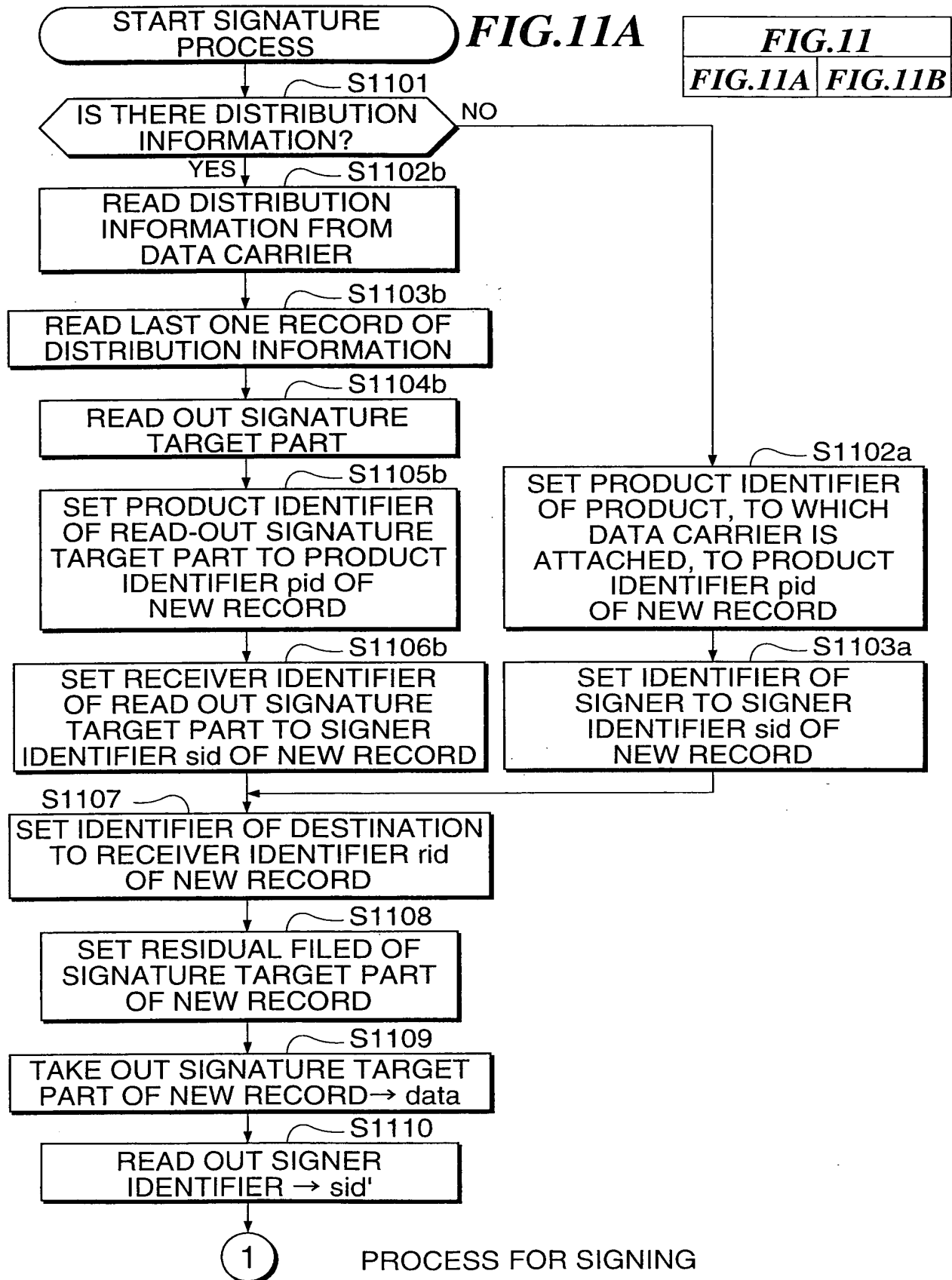
11/34

FIG.10B





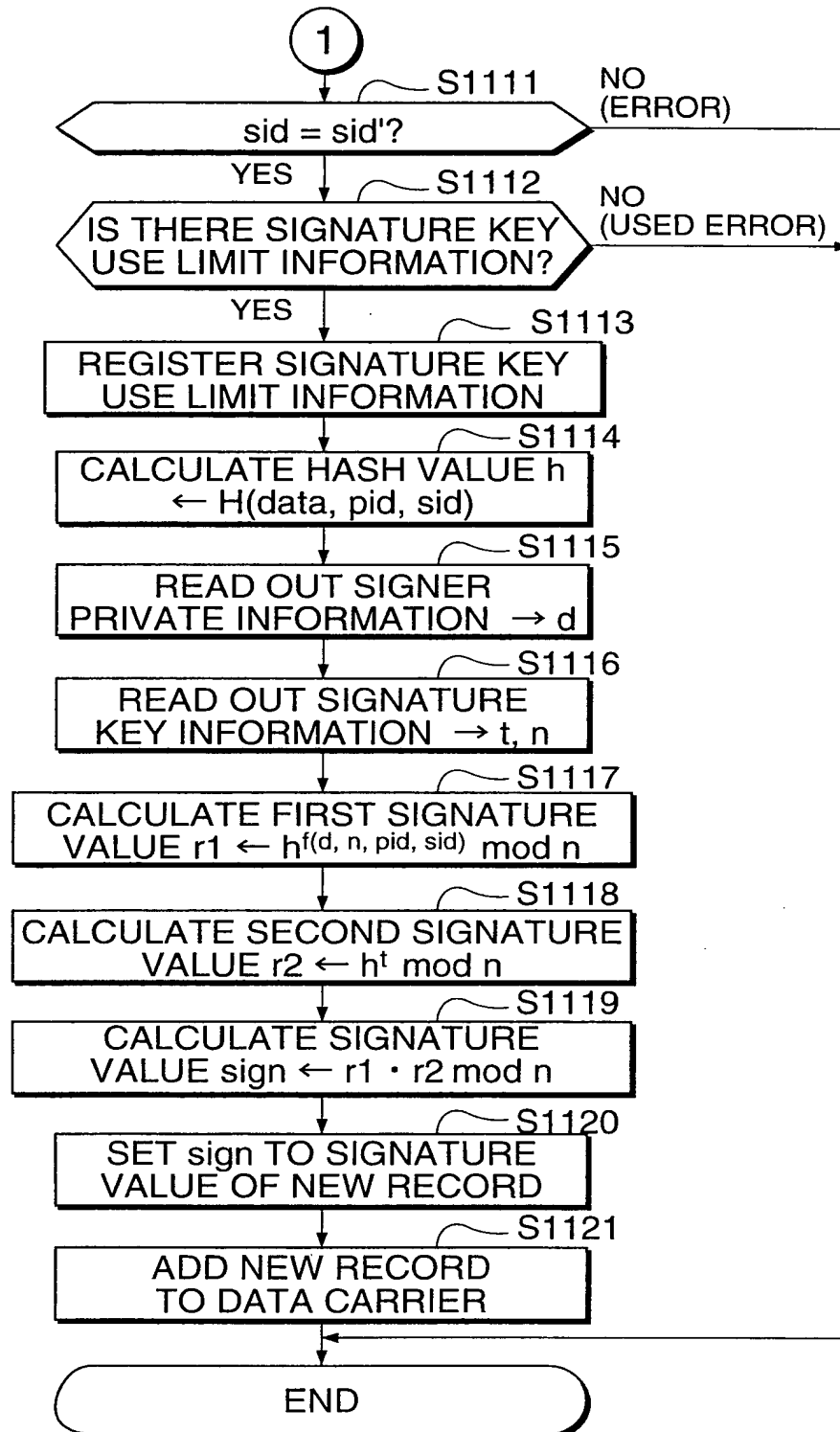
12/34





13/34

FIG.11B



PROCESS FOR SIGNING





14/34

FIG.12

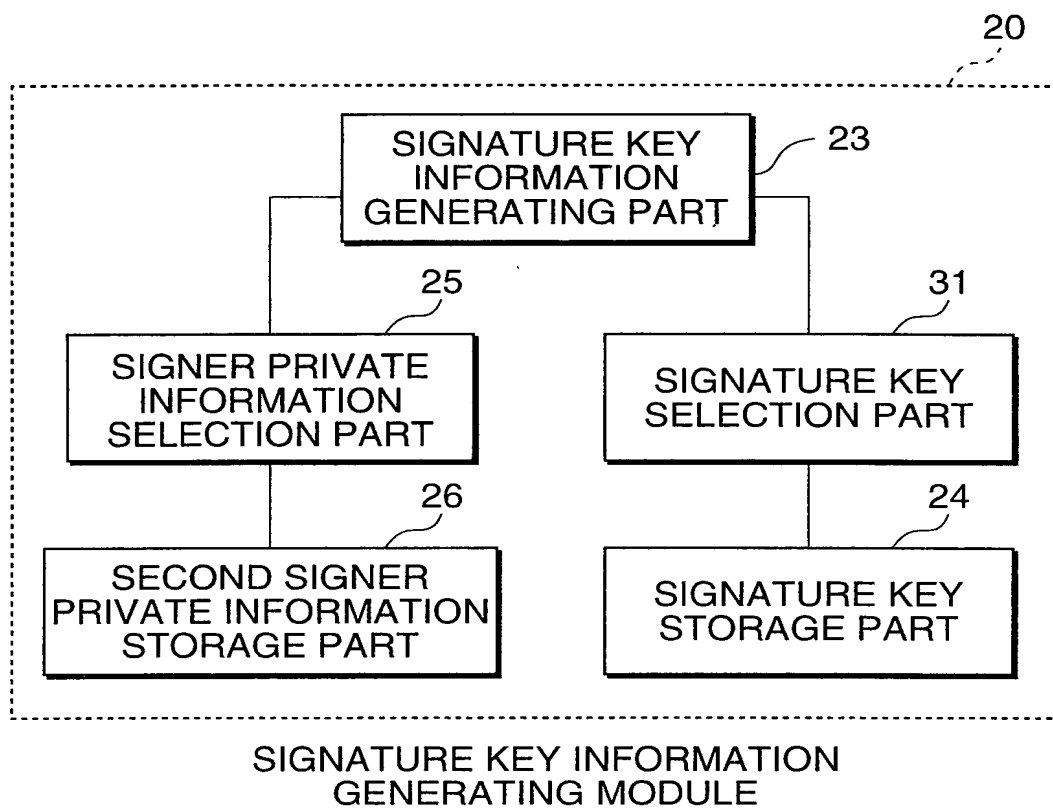
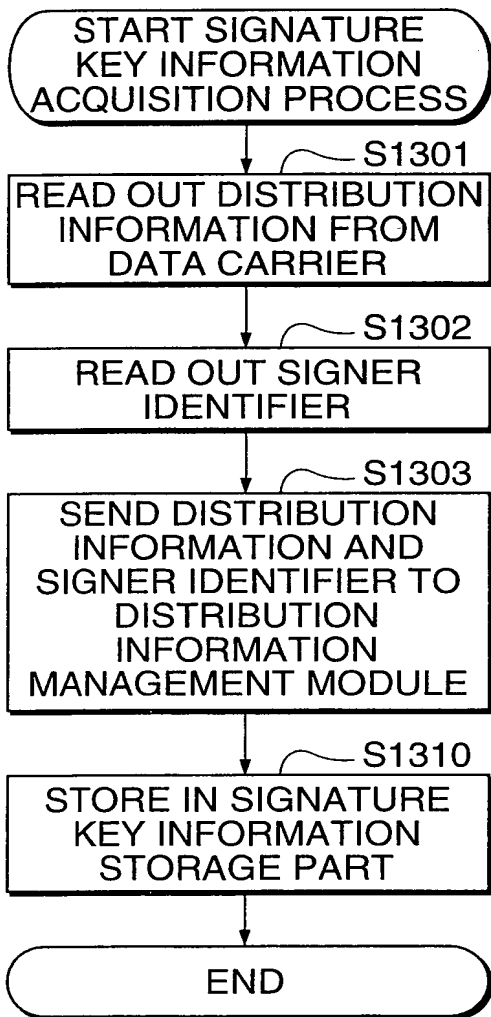
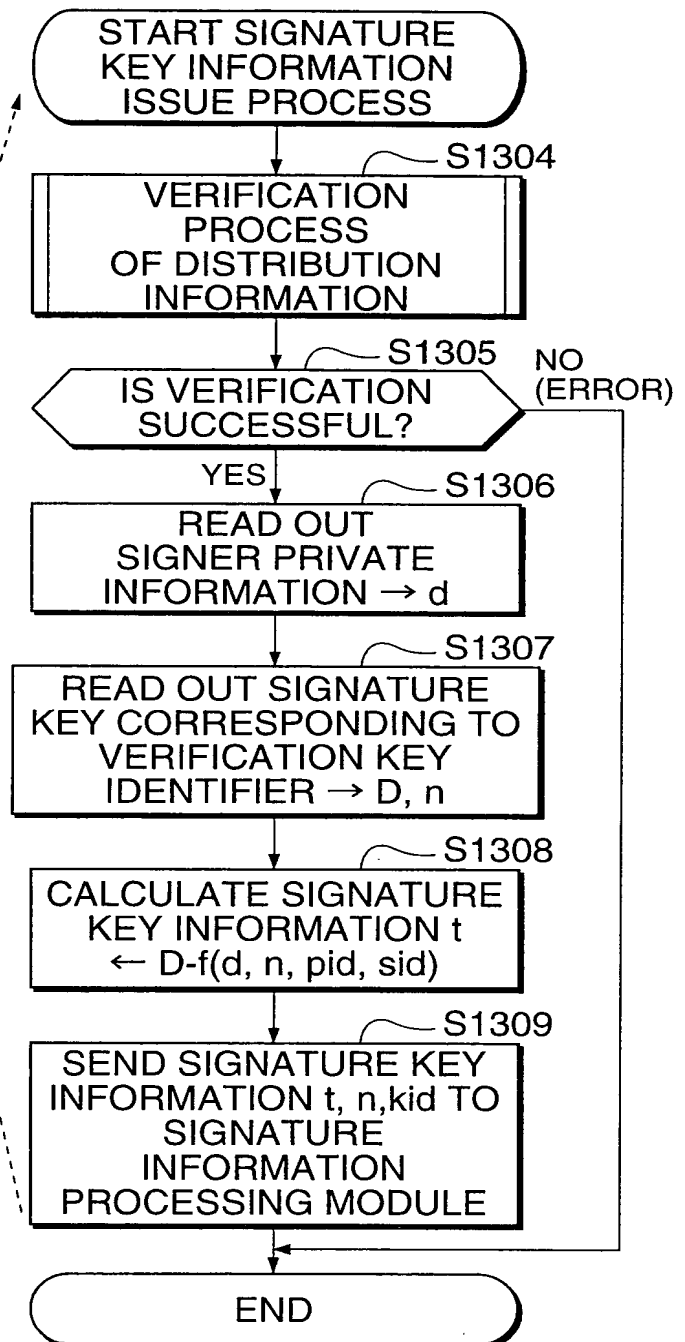


FIG.13A



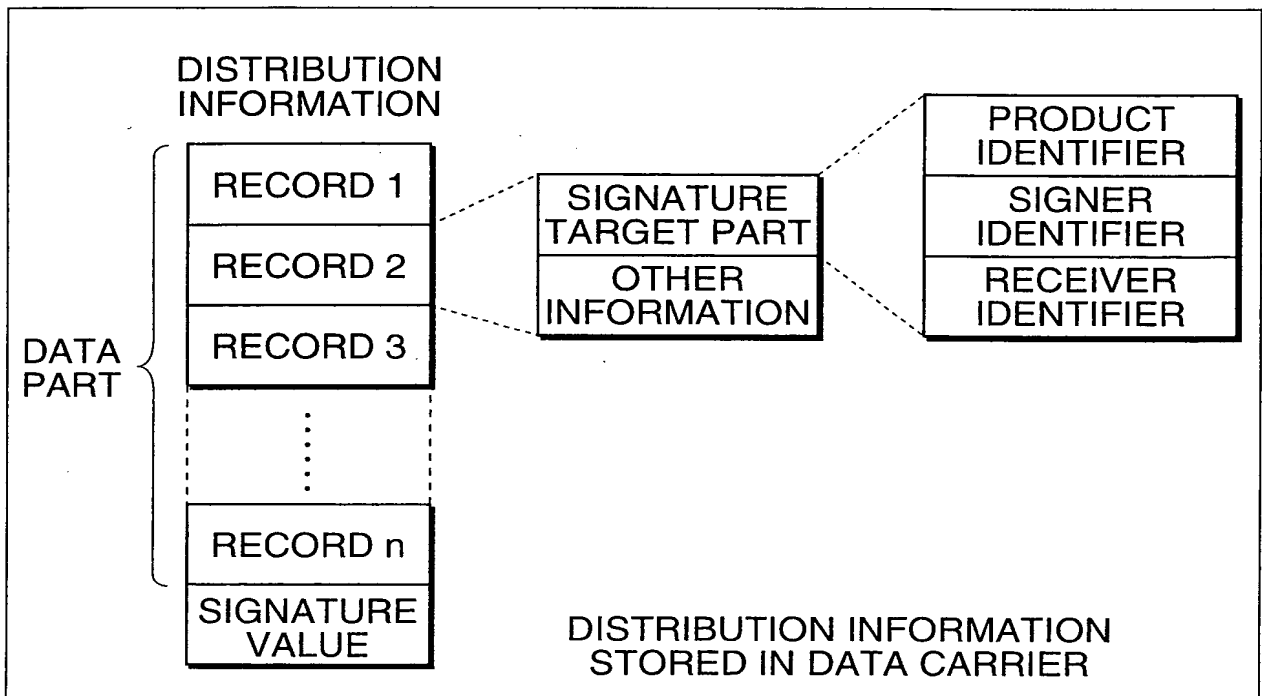
PROCESS FOR
SIGNATURE
KEY INFORMATION
ACQUISITION

FIG.13B



PROCESS FOR SIGNATURE KEY
INFORMATION ACQUISITION

FIG.14





17/34

FIG.15A

START SIGNATURE
VERIFICATION PROCESS

FIG.15
FIG.15A **FIG.15B**

$val \leftarrow 1$

READ OUT SIGNATURE
VERIFICATION KEY FROM
SIGNATURE VERIFICATION
KEY STORAGE PART $\rightarrow E, n$

READ OUT DATA PART
FROM DISTRIBUTION
INFORMATION

READ OUT ONE RECORD
FROM DATA PART

TAKE OUT SIGNATURE
TARGET PART FROM
RECORD $\rightarrow data$

READ OUT PRODUCT
IDENTIFIER FROM
SIGNATURE TARGET
PART $\rightarrow pid$

READ OUT SIGNER
IDENTIFIER FROM
SIGNATURE TARGET
PART $\rightarrow sid$

CALCULATE HASH
VALUE $h \leftarrow H(data, pid, sid)$

$val \leftarrow (val \cdot h) \bmod n$

IS THERE
UNPROCESSED RECORD
IN DATA PART?

YES

NO

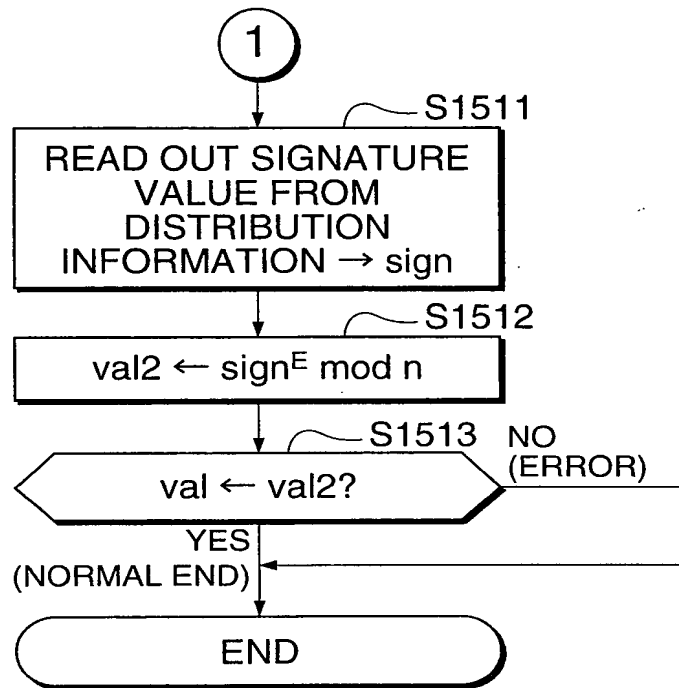
1

SIGNATURE
VERIFICATION
PROCESS IN
THE CASE WHERE
THERE IS ONLY
ONE SIGNATURE
VALUE IN DATA
CARRIER



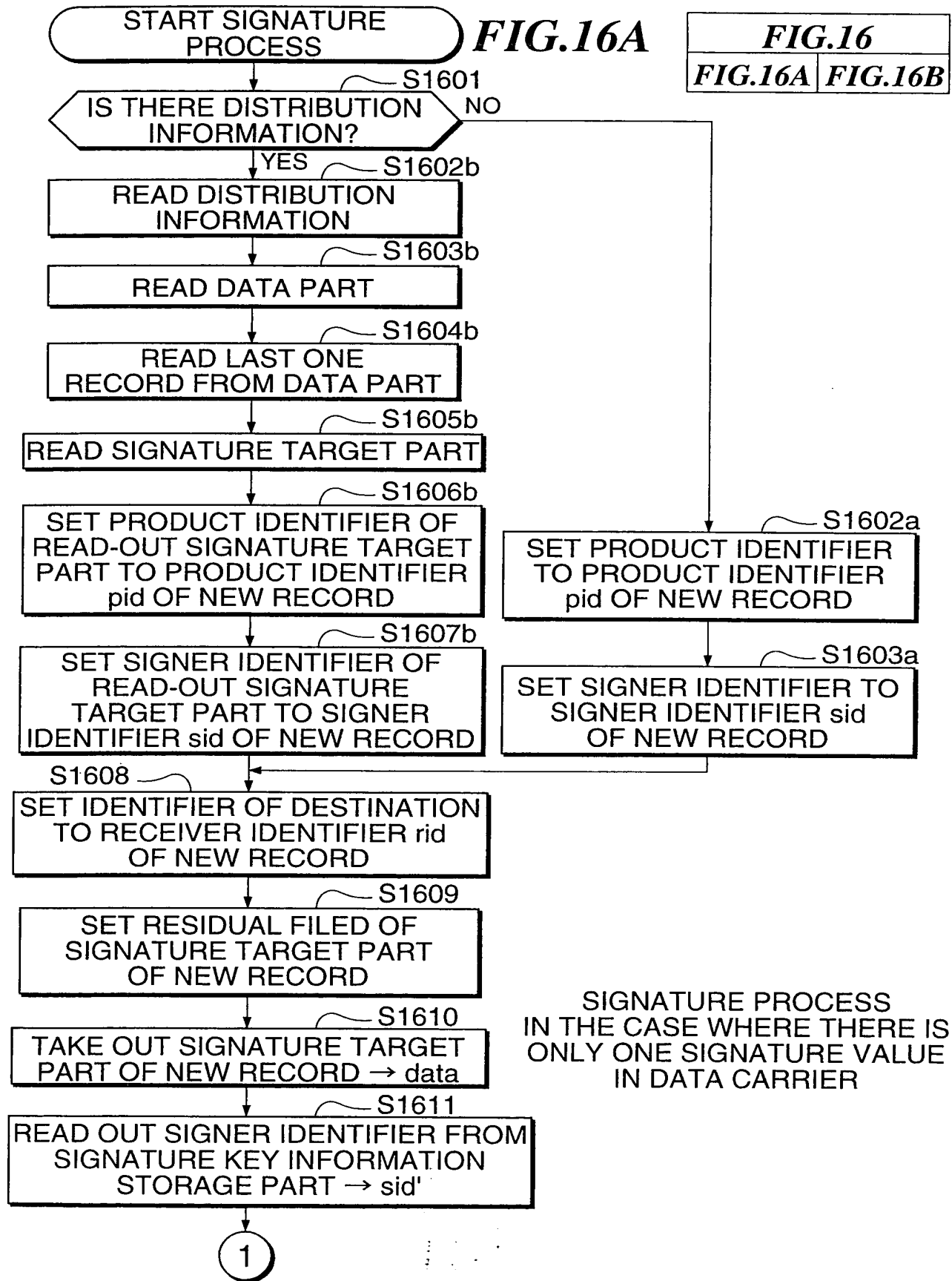
18/34

FIG.15B



SIGNATURE
VERIFICATION
PROCESSIN.
THE CASE WHERE
THERE IS ONLY
ONE SIGNATURE
VALUE IN DATA
CARRIER

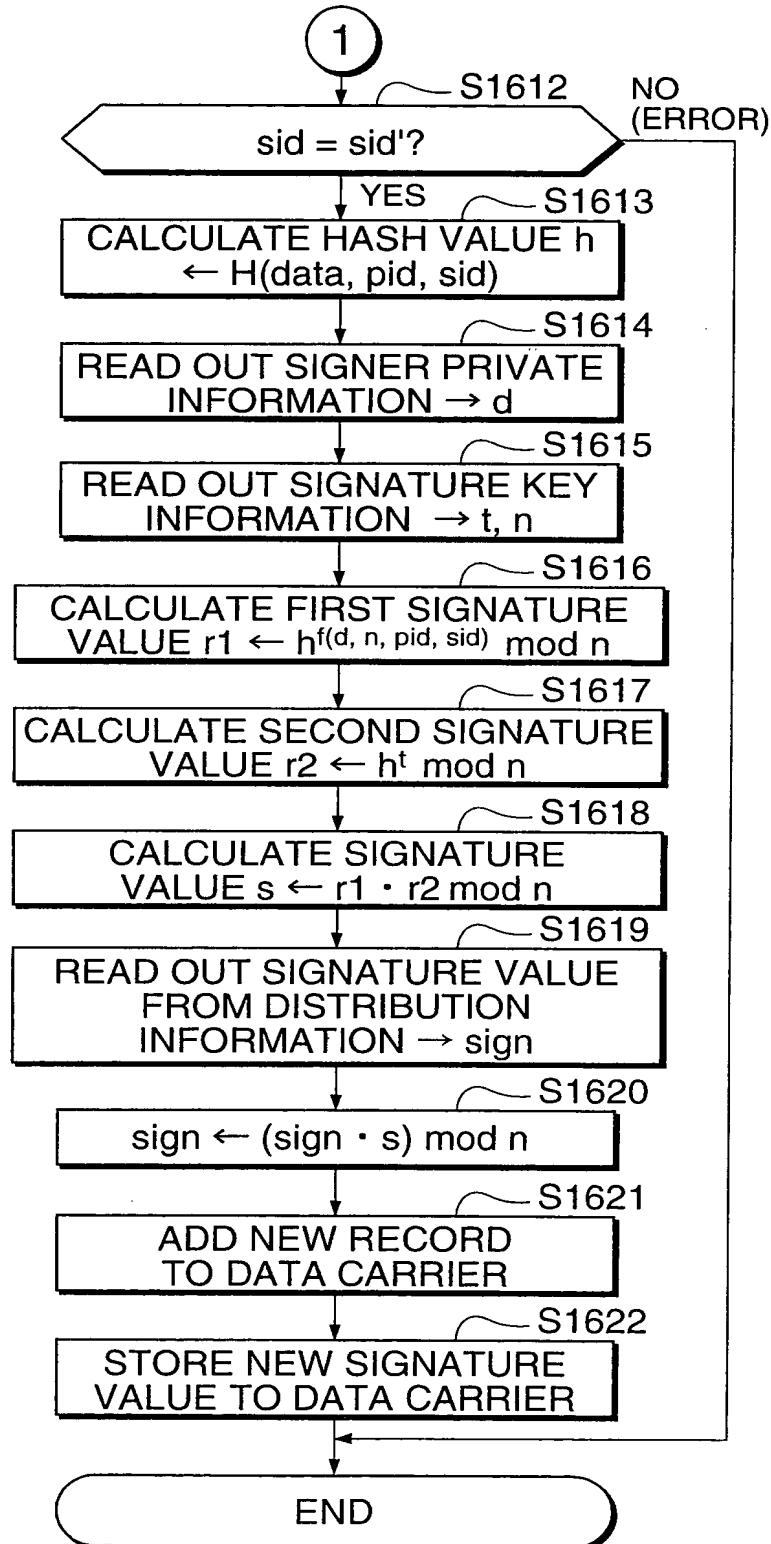






20/34

FIG.16B



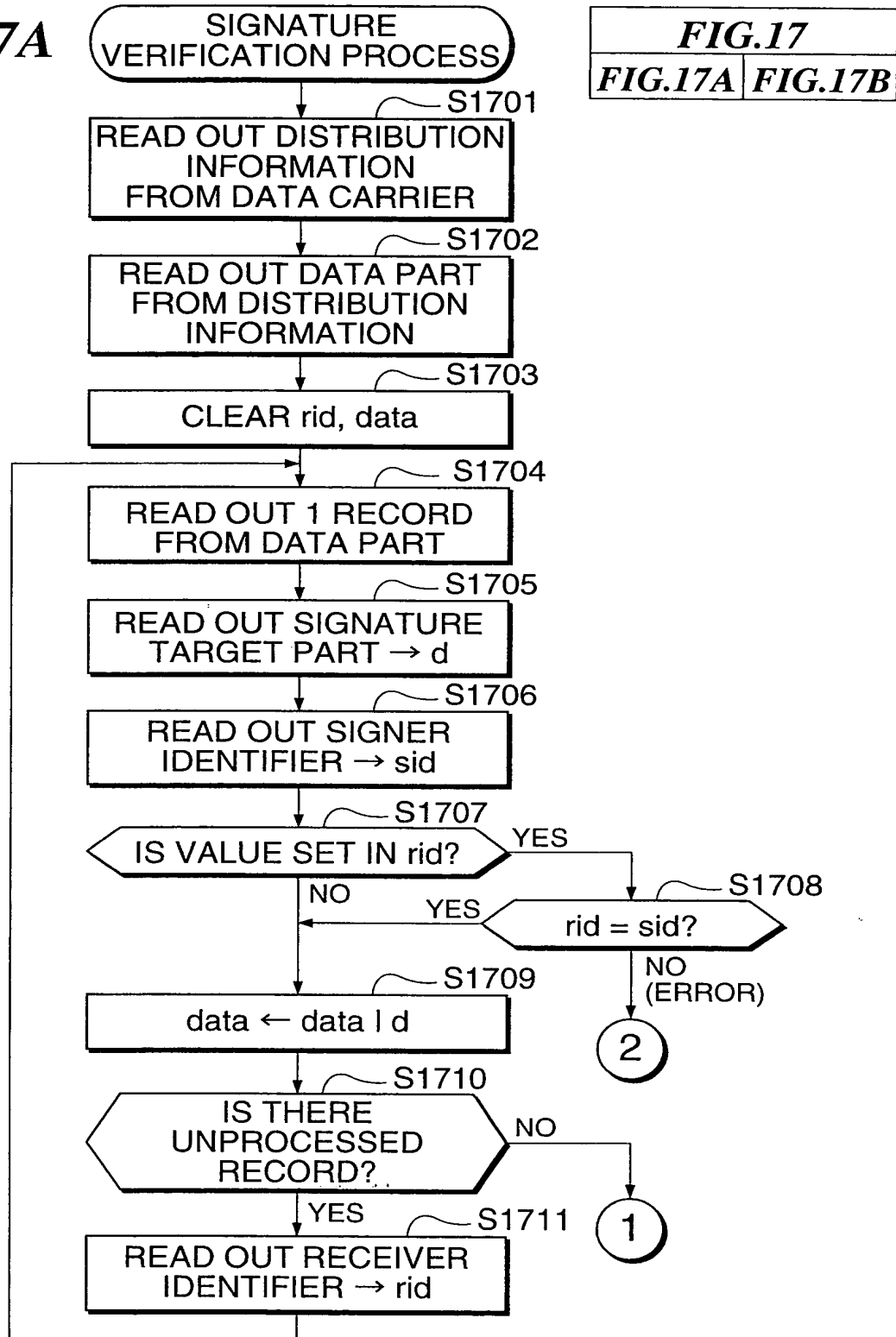
SIGNATURE PROCESS IN THE CASE WHERE THERE IS ONLY ONE SIGNATURE VALUE IN DATA CARRIER





21/34

FIG.17A



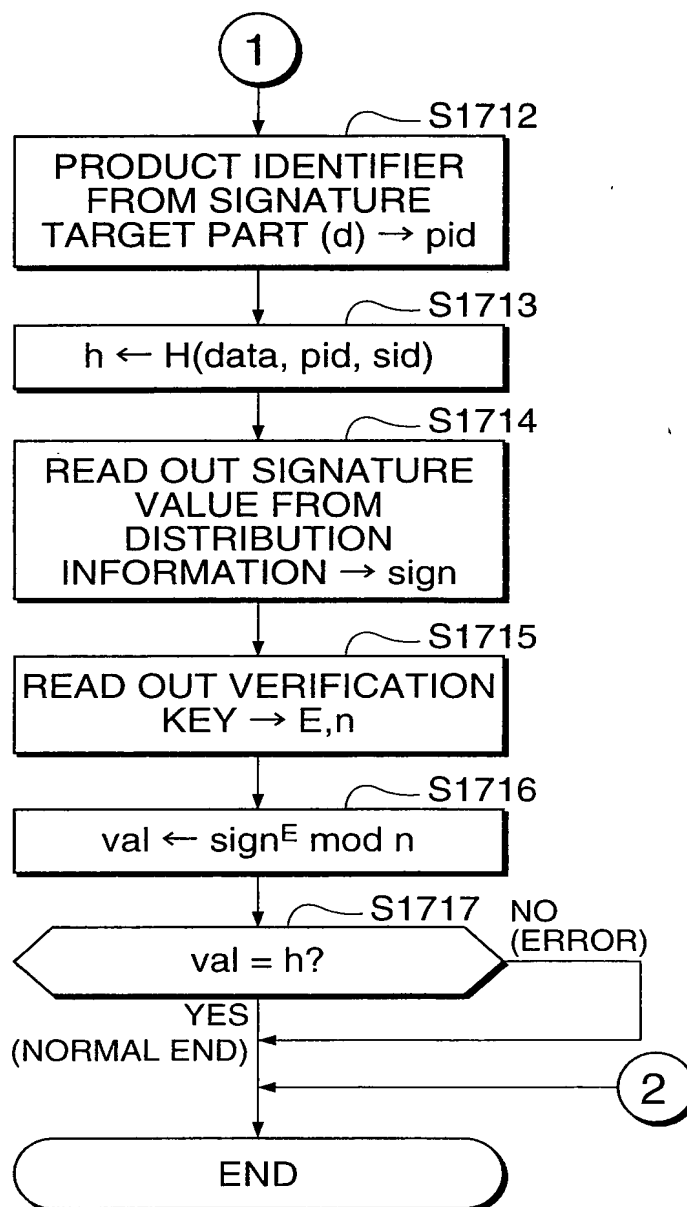
VERIFICATION PROCESS IN THE CASE
WHERE SIGNATURE IS ADDED TO THE WHOLE
(ONE VERIFICATION KEY)





22/34

FIG.17B



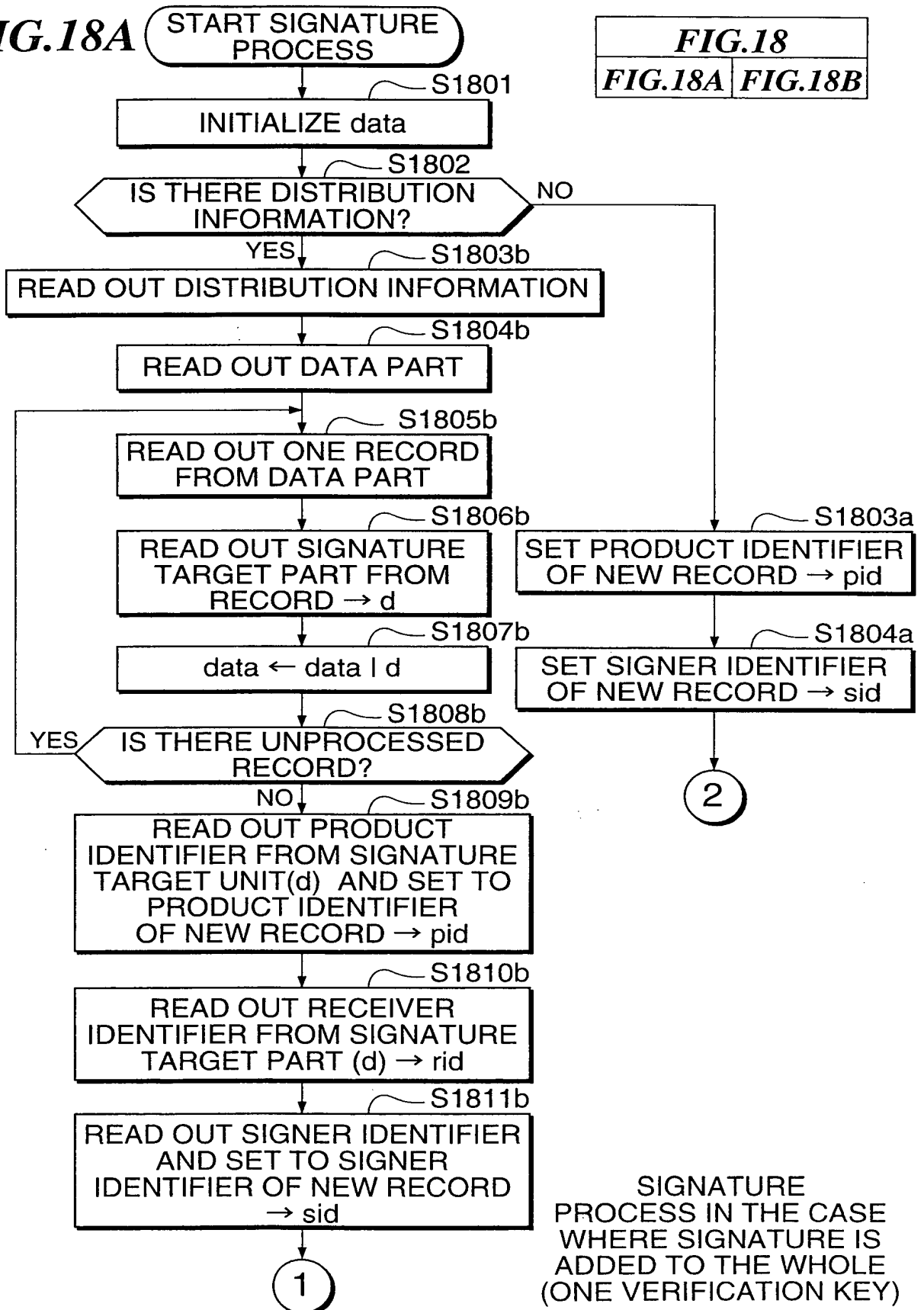
VERIFICATION PROCESS IN THE CASE
WHERE SIGNATURE IS ADDED TO THE WHOLE
(ONE VERIFICATION KEY)





23/34

FIG.18A





24/34

FIG.18B

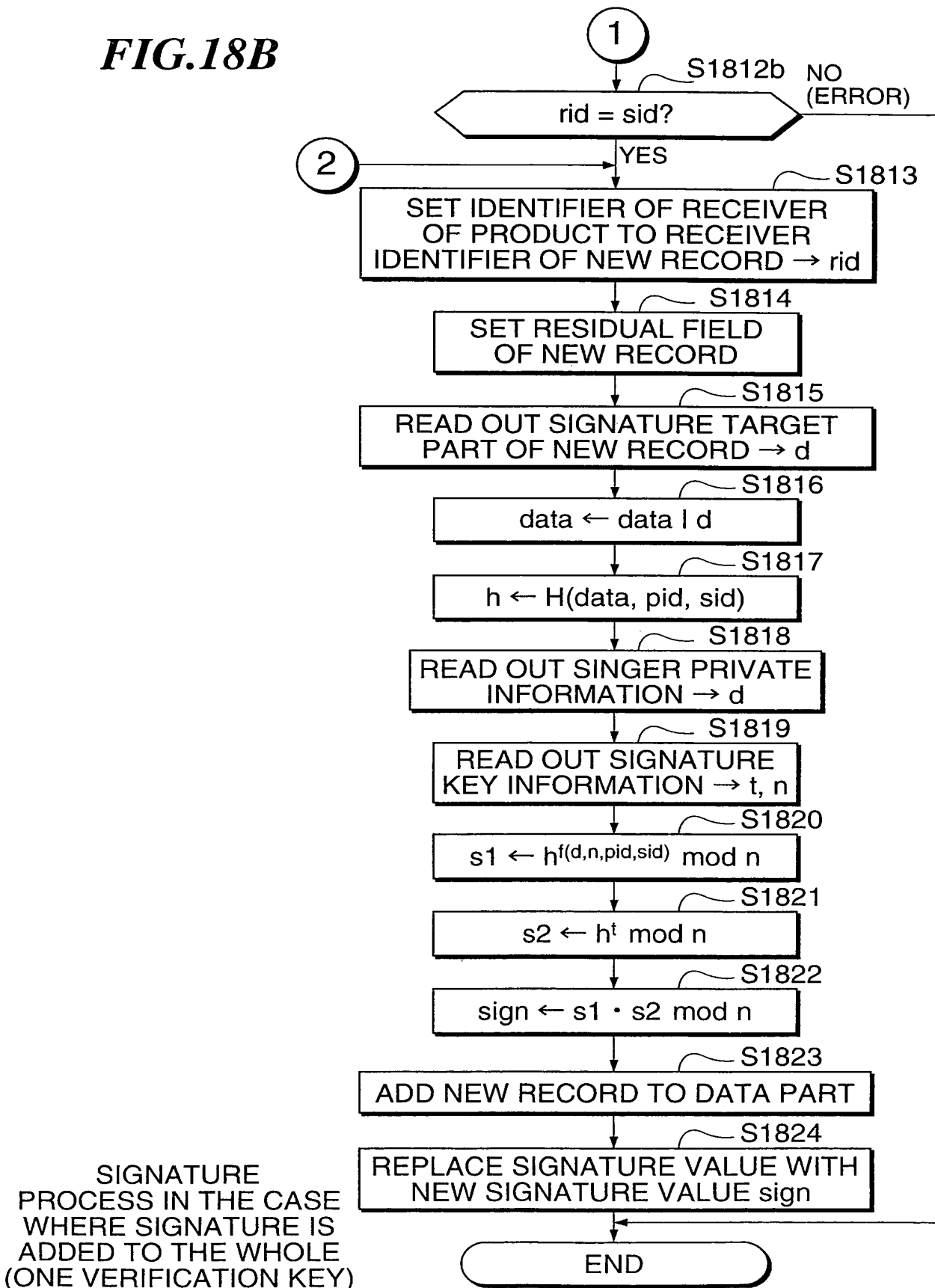
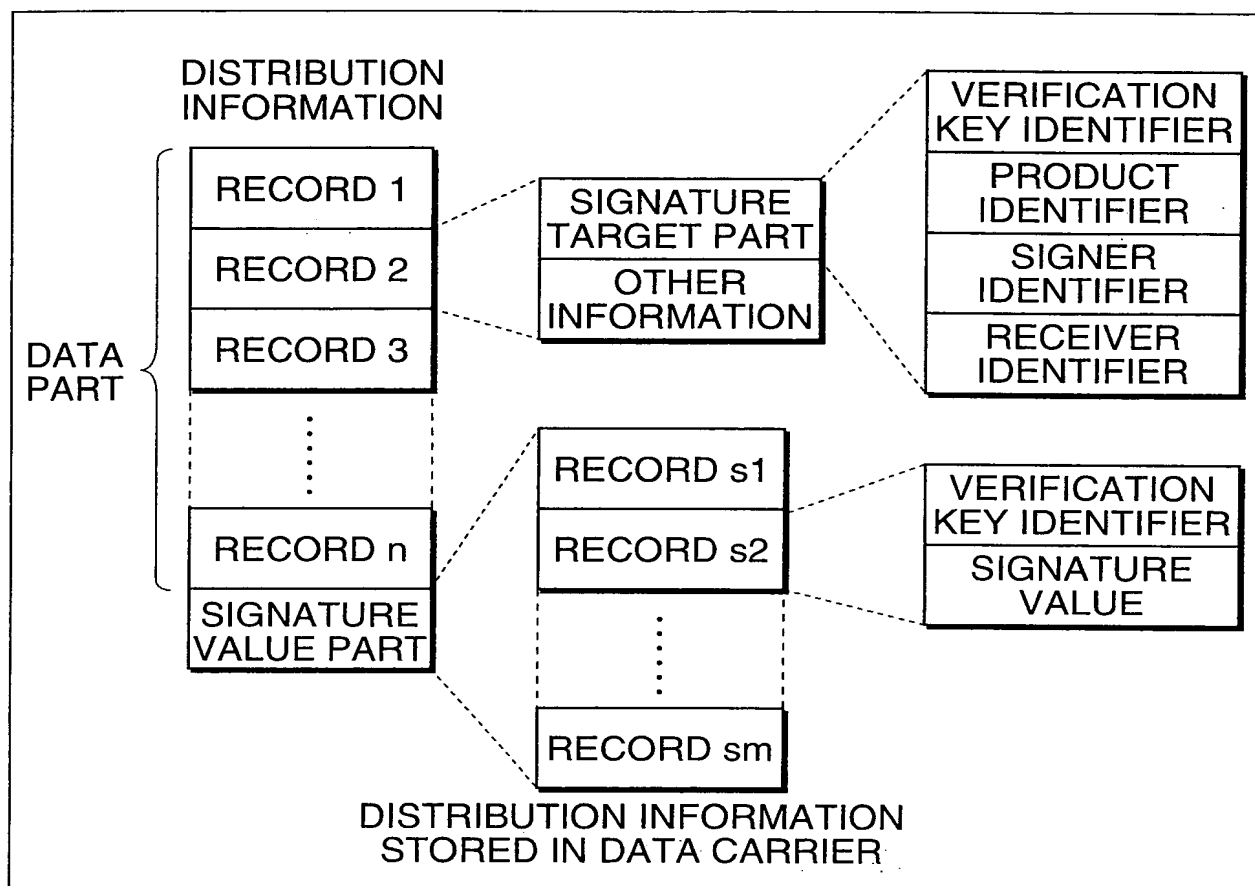


FIG.19

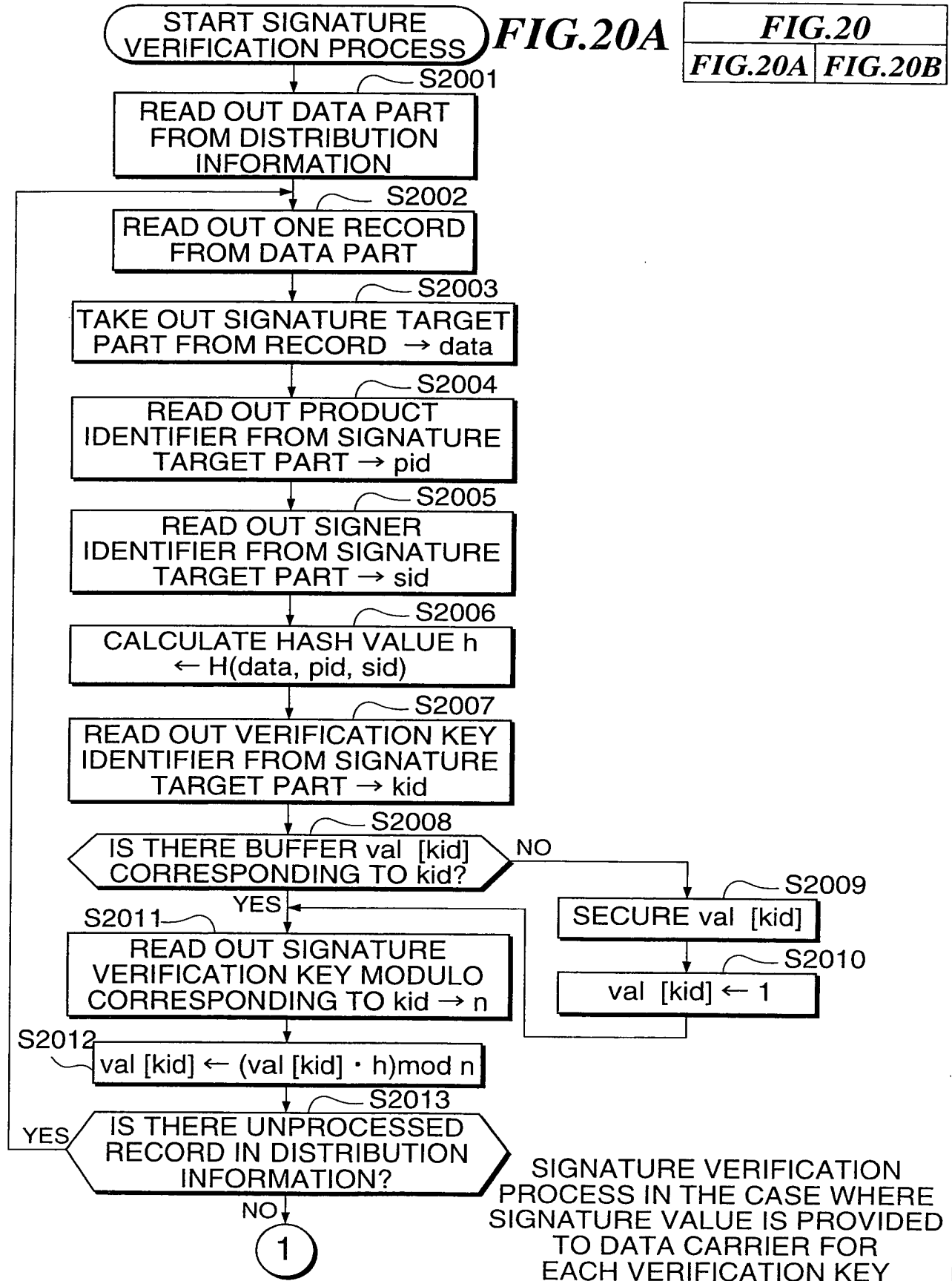


26/34

FIG.20A

FIG.20

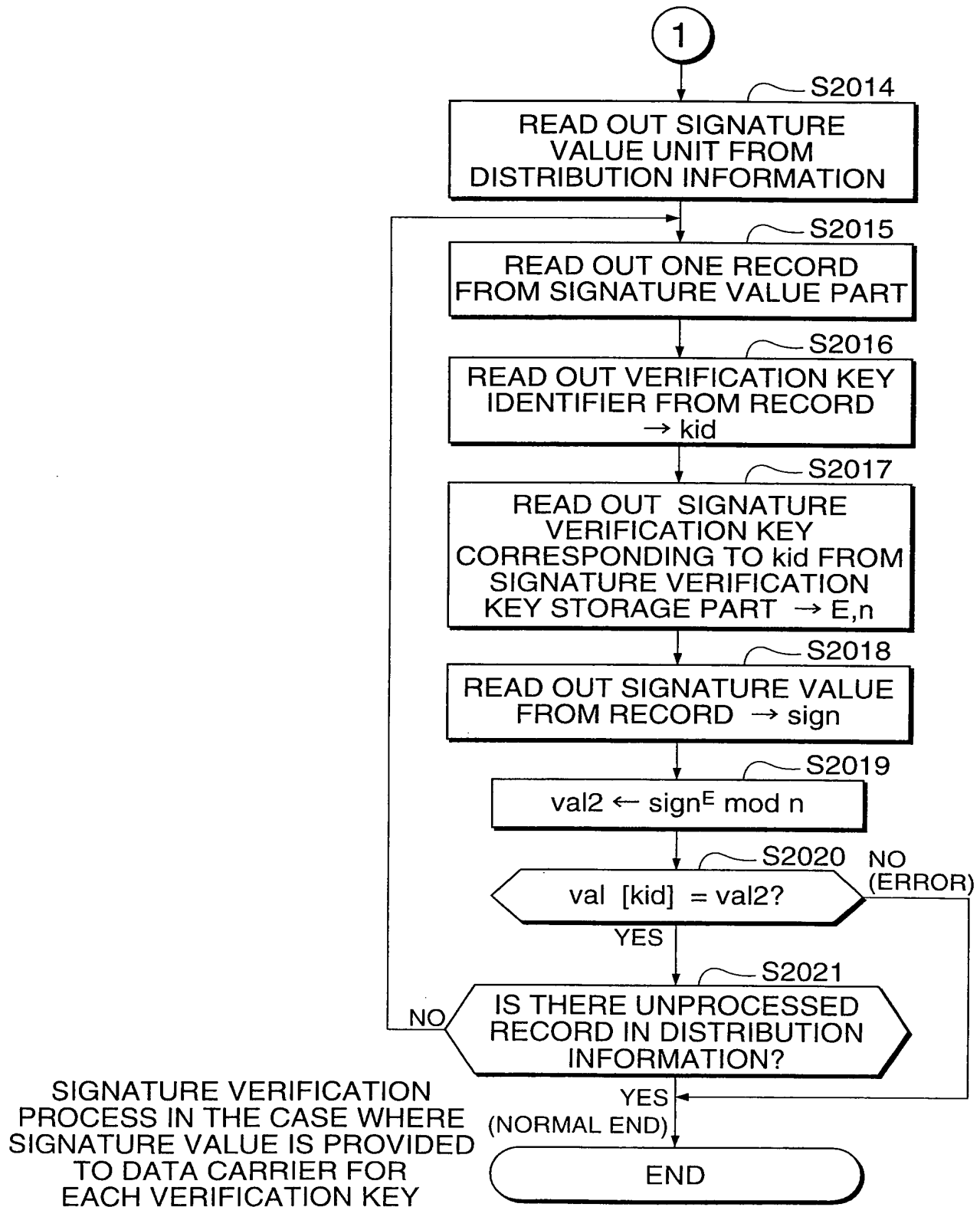
FIG.20A FIG.20B





27/34

FIG.20B





28/34

FIG.21A

START SIGNATURE
PROCESS

FIG.21

FIG.21A **FIG.21B**

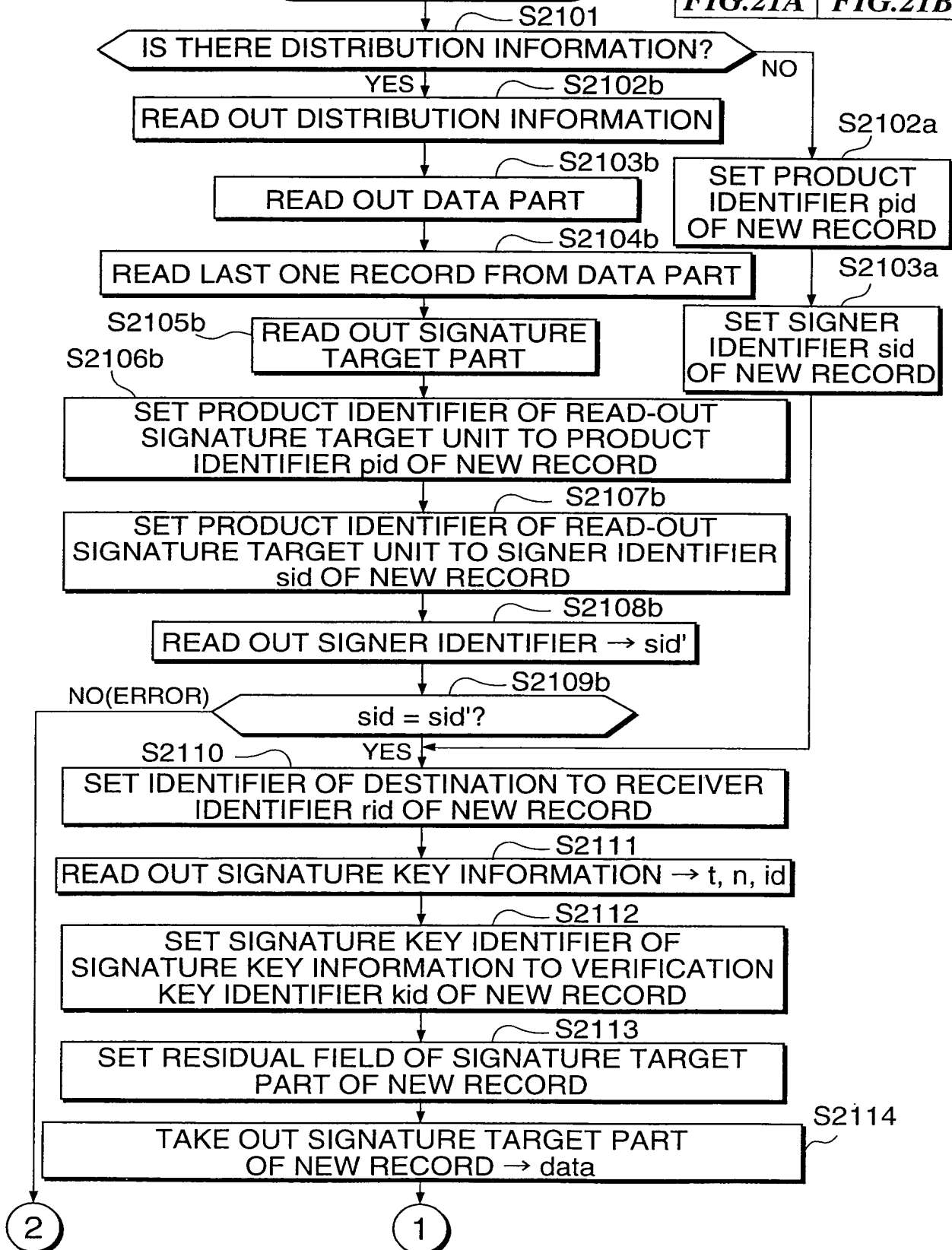
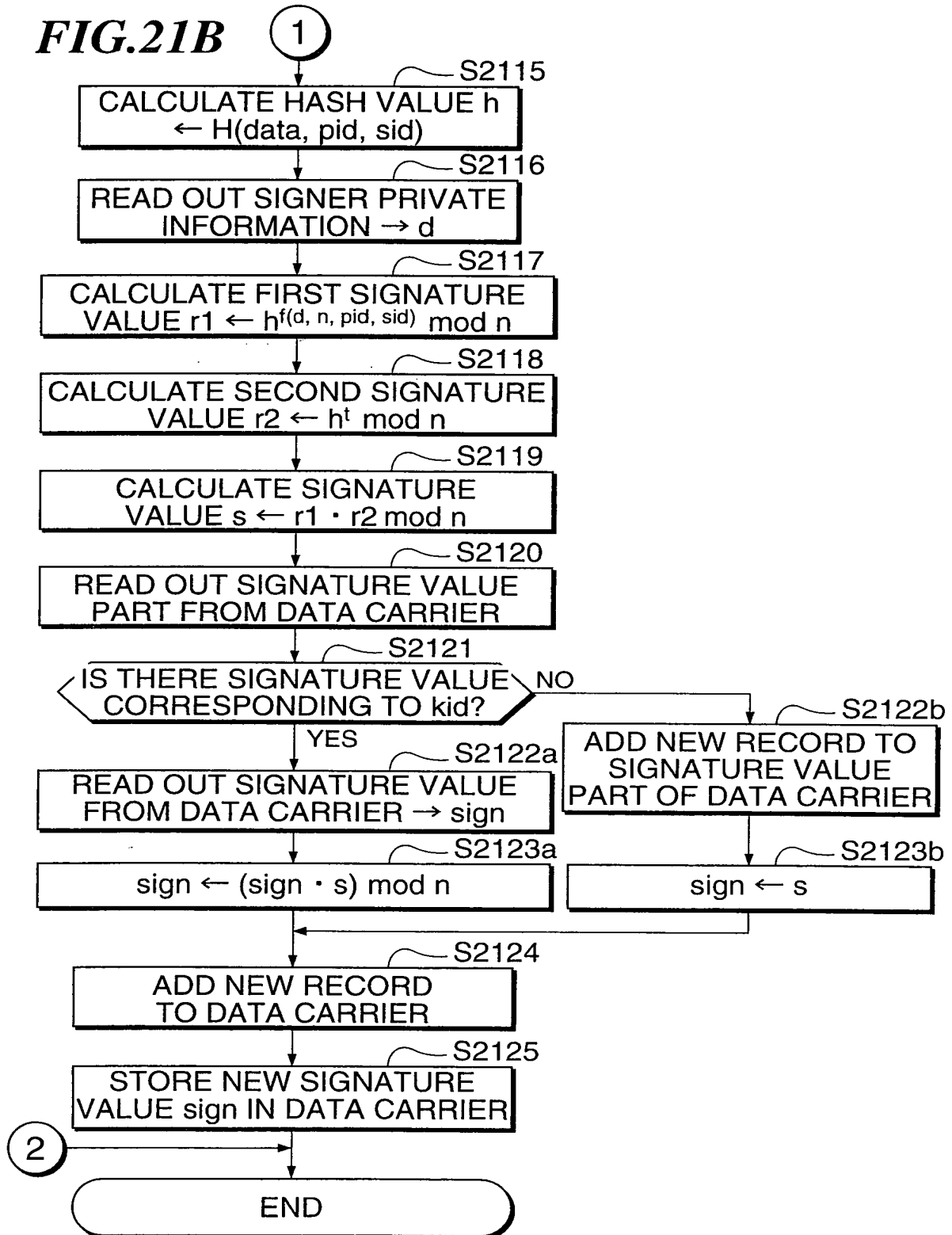


FIG.21B



SIGNATURE PROCESS IN THE CASE WHERE
SIGNATURE VALUE IS PROVIDED IN DATA
CARRIER FOR EACH VERIFICATION KEY



30/34

FIG.22A

**SIGNATURE
VERIFICATION PROCESS**

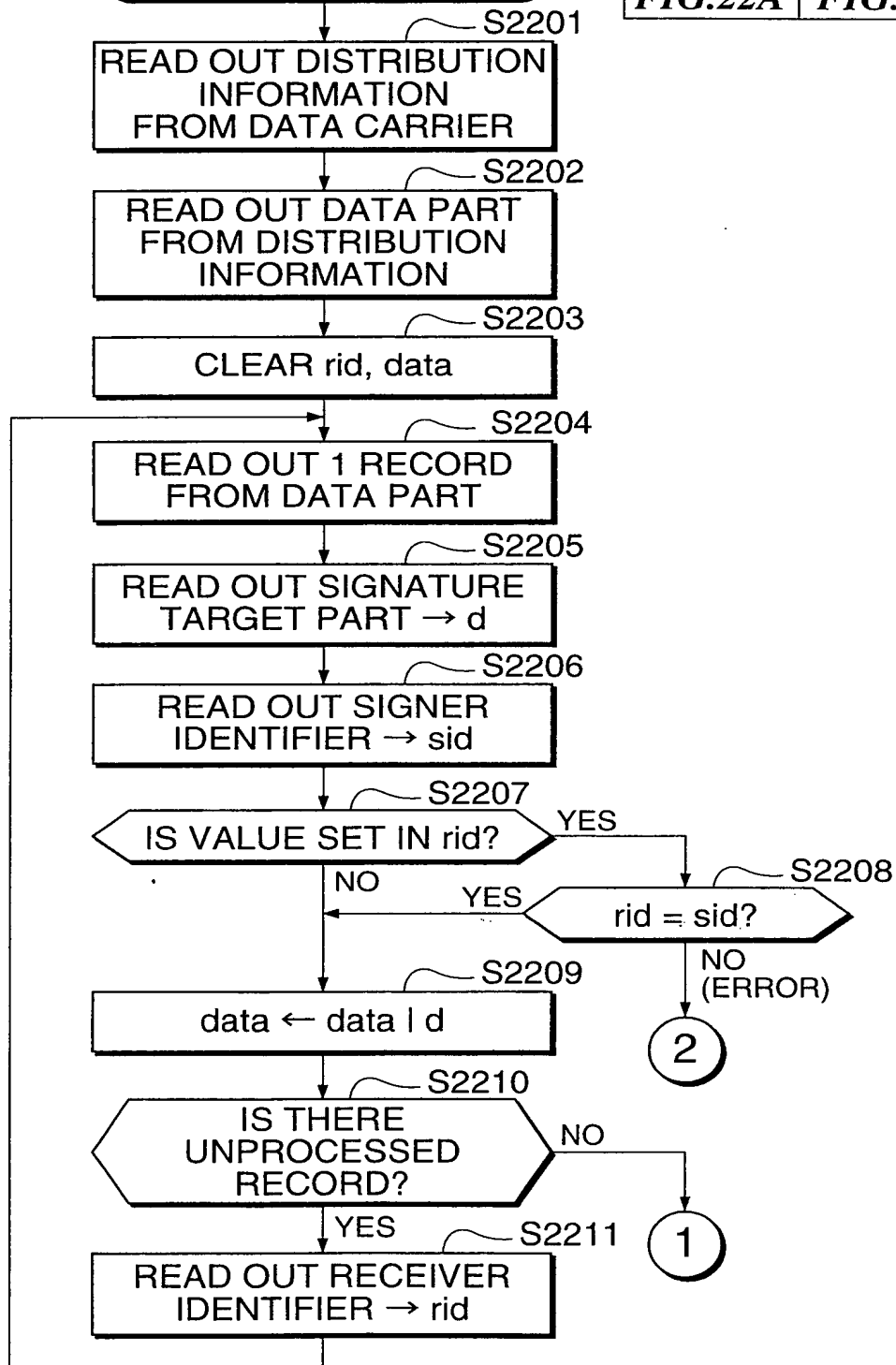


FIG.22
FIG.22A | **FIG.22B**

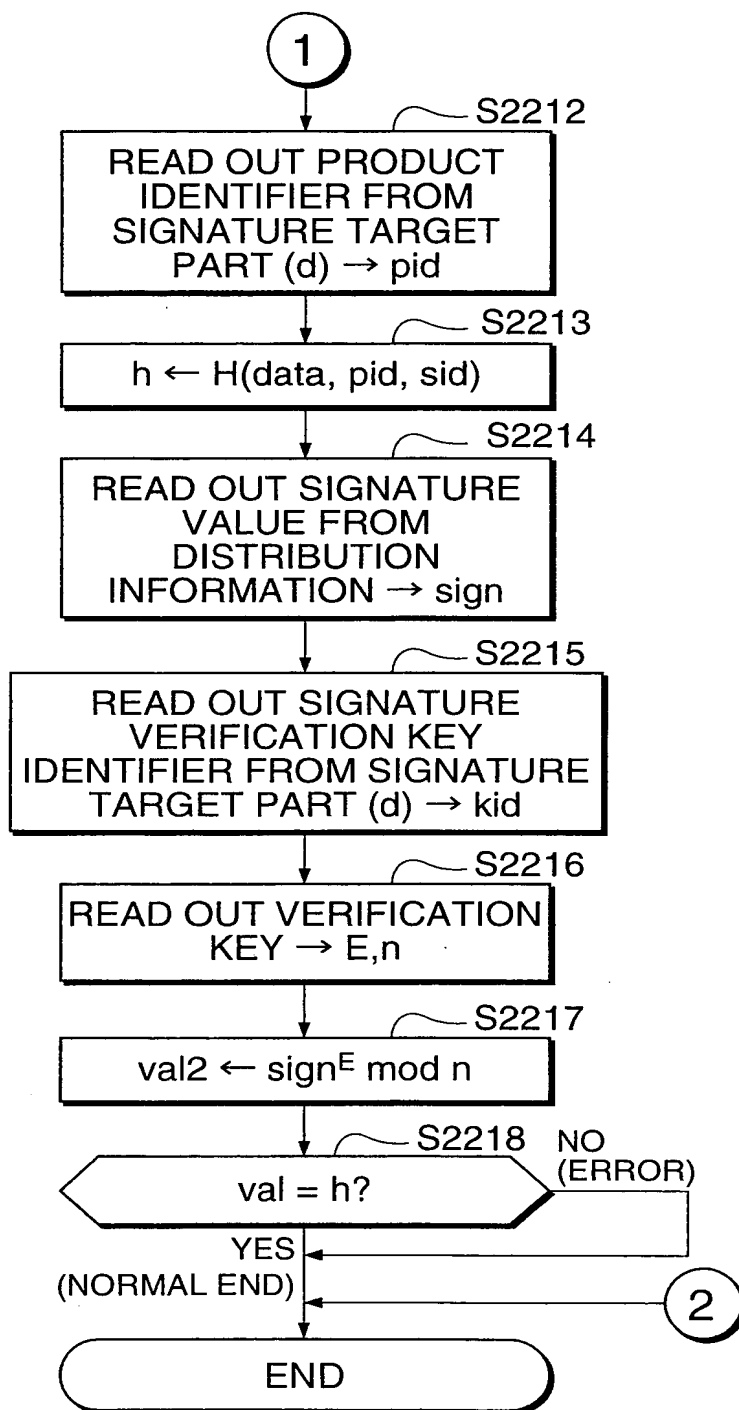
VERIFICATION PROCESS IN THE CASE
WHERE SIGNATURE IS ADDED TO THE WHOLE
(PLURAL VERIFICATION KEYS)





31/34

FIG.22B



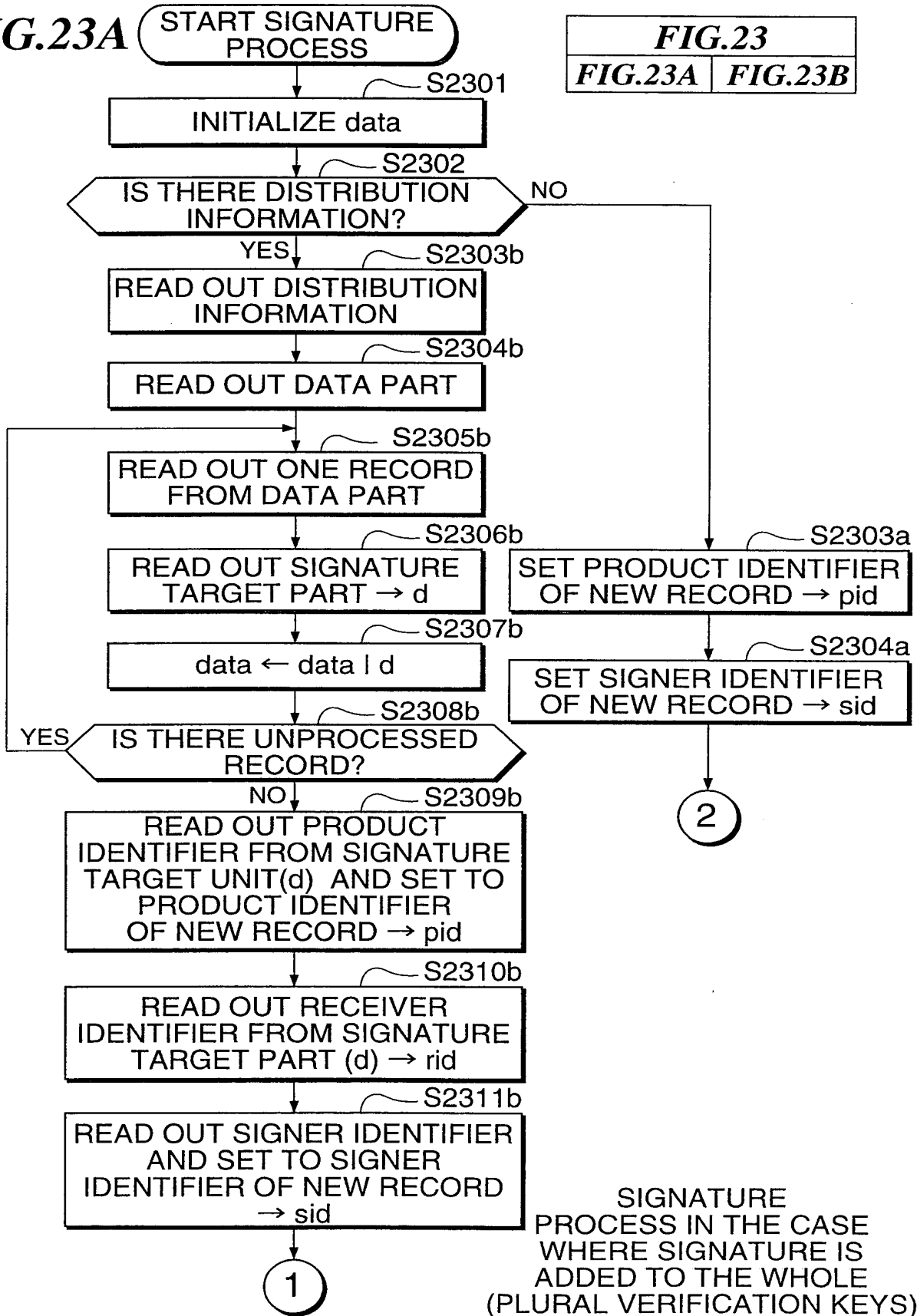
VERIFICATION PROCESS IN THE CASE
WHERE SIGNATURE IS ADDED TO THE WHOLE
(PLURAL VERIFICATION KEYS)





32/34

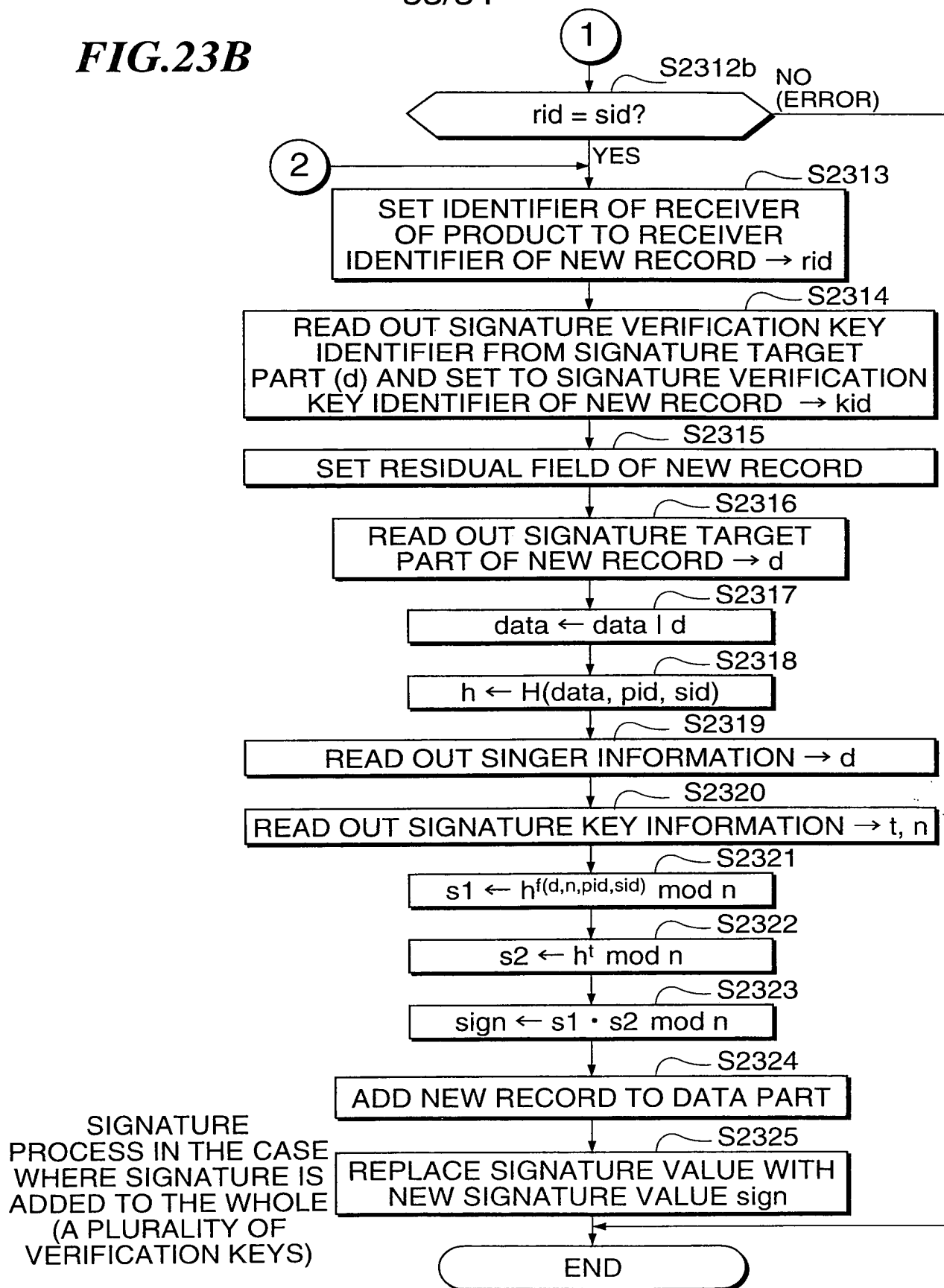
FIG.23A





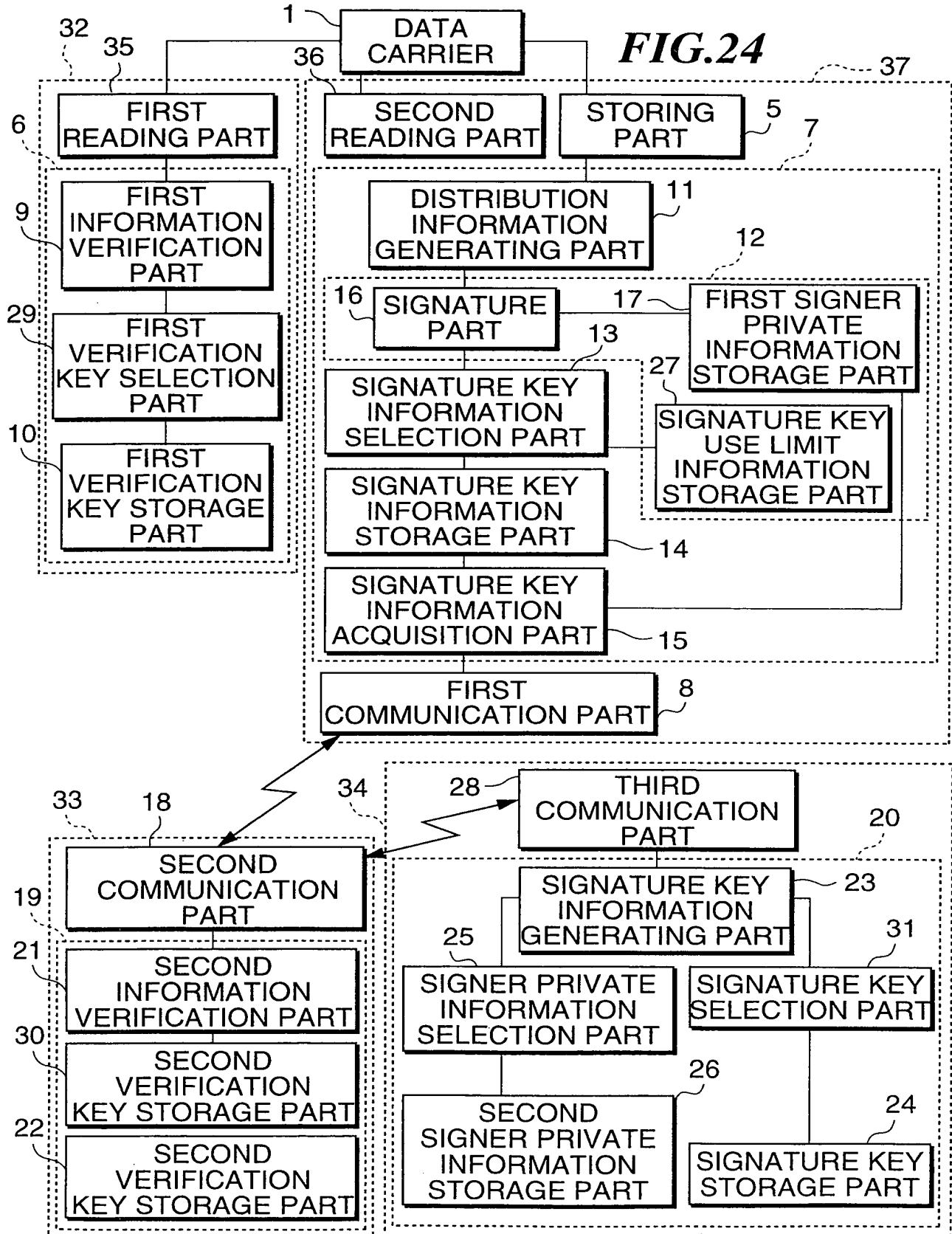
33/34

FIG.23B



34/34

FIG.24



STRUCTURE OF MODIFIED EXAMPLE